Module 3:Attacking the Foundation – IP, TCP & UDP Vulnerabilities

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: **KUDZAISHE MAJEZA**

Agenda

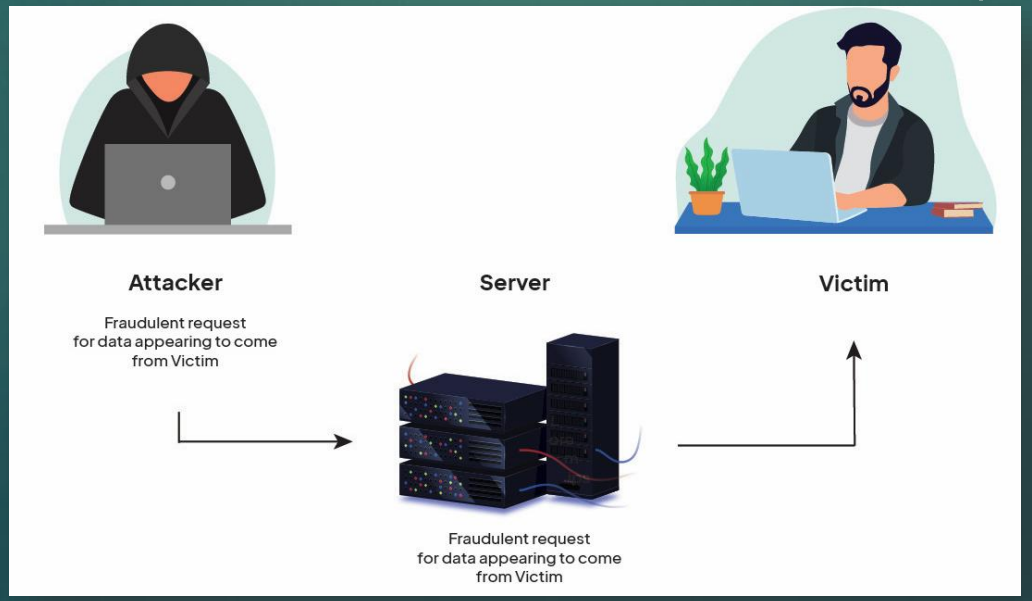
- Introduction to Protocol Vulnerabilities
- IP Protocol Vulnerablities
- More IP Vulnerabilities
- TCP Vulnerabilities
- More TCP Weaknesses
- UDP Vulnerabilities
- More UDP Weaknesses
- Why These Vulnerabilities Matter
- Real-Life Example: UDP Amplification Attack (2024–2025)
- How to Defend Against These Attacks
- Summary & Key Takeaways

Introduction

- Core internet protocols (IP, TCP, UDP) were not originally built with security in mind.
- Attackers frequently exploit weaknesses at these foundational layers.
- Understanding protocol vulnerabilities is essential for preventing low-level network attacks.

IP Protocol Vulnerabilities

- **IP Spoofing** – attackers forge the source IP to hide identity.
- **Fragmentation Attacks** – maliciously crafted fragments bypass firewalls & IDS.
- **ICMP Misuse** – smurf attacks, ping floods, reconnaissance scanning.
- **No authentication** built into IP → attacker can easily impersonate hosts.

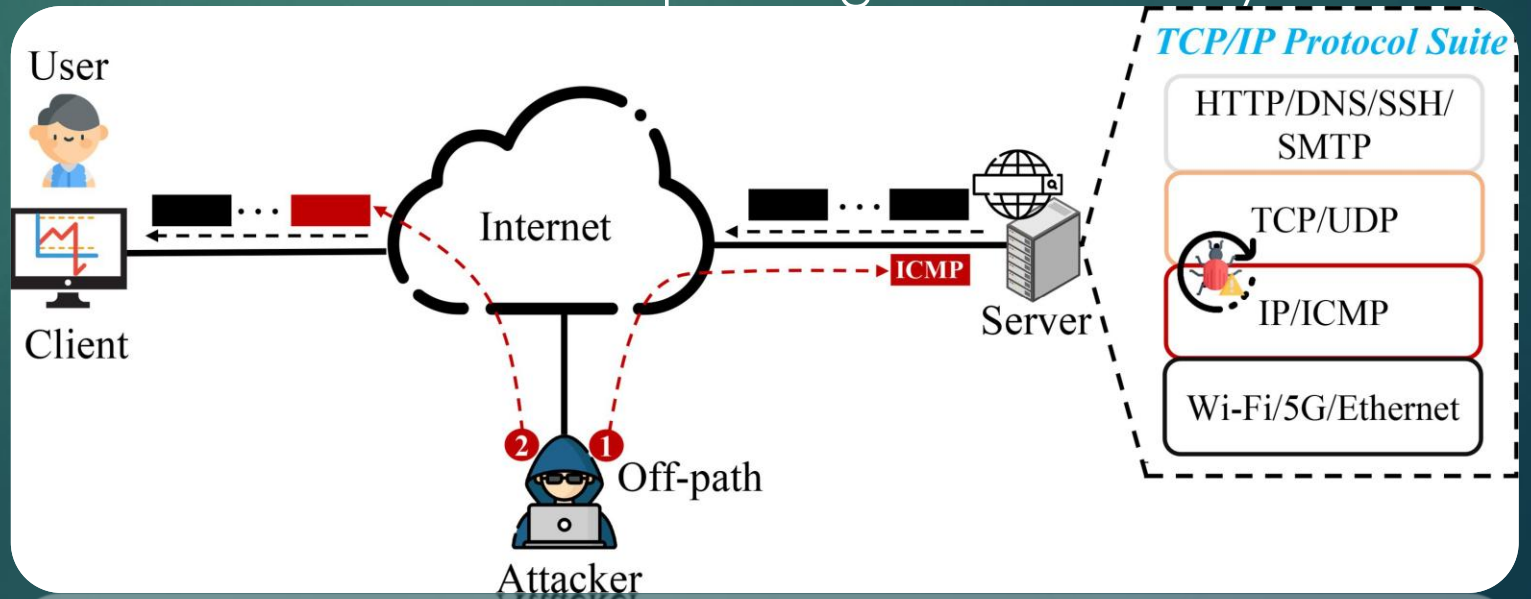


More IP Vulnerabilities

- **Source routing manipulation** – attacker controls packet path.
- **IP options field exploitation** – used to bypass security devices.
- **IP scanning attacks** – enumeration of live hosts for later attacks.

TCP Vulnerabilities

- **TCP SYN Flood** – overwhelms the server with half-open sessions.
- **Session Hijacking** – attacker predicts session sequence numbers and takes over.
- **TCP Reset Attack (RST Flood)** – forged RST packets terminate sessions.
- **Sequence Number Prediction Attack** – manipulating TCP's reliability mechanism.

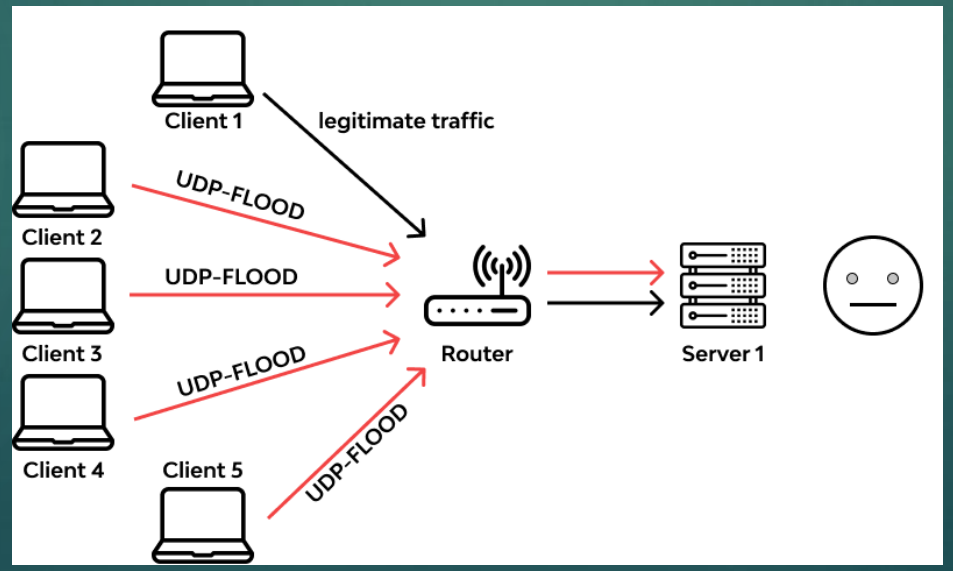


More TCP Weaknesses

- **ACK Storms** – attackers force endless ACK loops.
- **Man-in-the-Middle attacks** on unencrypted sessions.
- **TCP Replay Attacks** – re-sending previously captured packets.

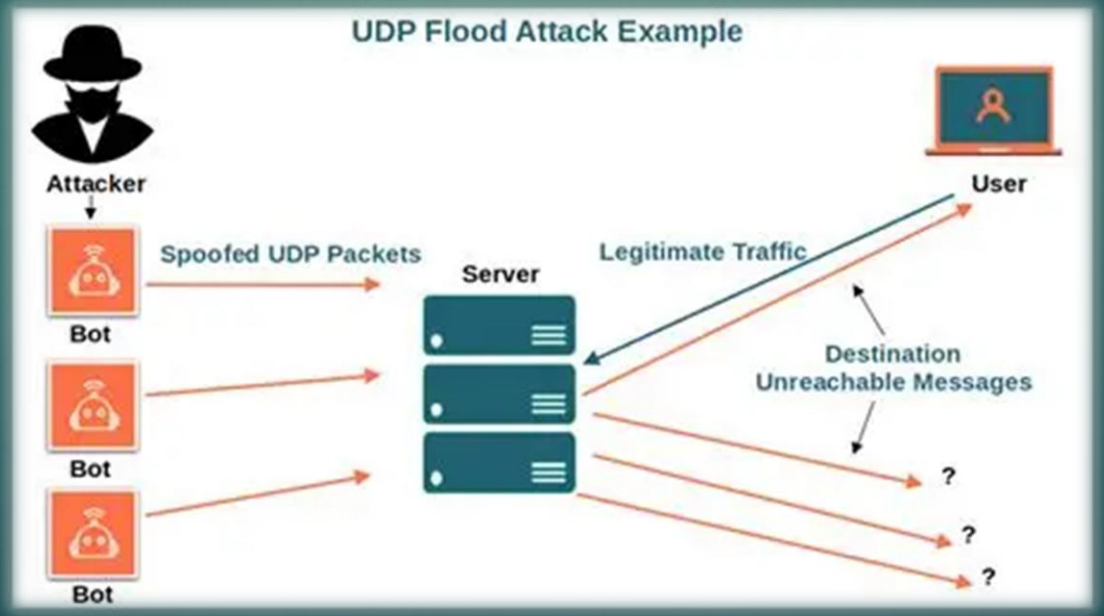
UDP Vulnerabilities

- **UDP Amplification** – used in massive DDoS attacks (DNS, NTP, CLDAP).
- **Connectionless & Stateless** – no handshake → easy spoofing.
- **No congestion control** – vulnerable to traffic flooding.
- **Reflection Attacks** – attacker bounces traffic through vulnerable servers.



More UDP Weaknesses

- **VoIP & streaming protocols** can be abused for DoS attacks.
- **UDP scanning** – attackers identify open services through crafted probes.
- **Tunneling attacks** – UDP often used to bypass firewalls (e.g., VPN misuse).



Why These Vulnerabilities Matter

- Attacks disrupt entire networks and critical services.
- Even modern firewalls may struggle with low-level protocol attacks.
- Attackers rely heavily on spoofing, floods, and amplification in real-world breaches.
- Strong endpoint and network security requires understanding these weaknesses.

Real-Life Example: UDP Amplification Attack (2024–2025)

- A major **European telecom provider** suffered a **500+ Gbps DDoS attack**.
- Attackers used a **UDP amplification chain** involving DNS, NTP, and CLDAP servers.
- The attack overwhelmed backbone routers, causing **nationwide internet outages**.
- Shows how protocol-level vulnerabilities can cripple entire countries.

How to Defend Against These Attacks

- Implement **ingress/egress filtering** to stop spoofed traffic.
- Enable **rate limiting** for ICMP, UDP, and SYN packets.
- Deploy **stateful firewalls & intrusion detection systems**.
- Disable unused UDP/TCP services.
- Keep all networking devices patched and configured correctly.

Summary

- IP, TCP, and UDP have inherent vulnerabilities attackers exploit.
- Protocol-level attacks can disrupt entire networks.
- Security depends on correct configuration, monitoring, and filtering.
- Understanding foundational protocol weaknesses strengthens endpoint defense.