Module 3: Attacking the Foundation – IPv4 & IPv6

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: KUDZAISHE MAJEZA

Agenda

- Introduction to IPv4 and IPv6
- IPv4 Overview
- IPv4 Packet Header
- IPv4 Security Weaknesses
- IPv4 Real-Life Scenario
- IPv6 Overview
- IPv6 Packet Header
- IPv6 Security Strengths & Weaknesses
- IPv6 Real-Life Scenario
- IPv4 vs IPv6 Comparison
- IPv4 vs IPv6 in Attacks
- Summary & Key Takeaways

Introduction

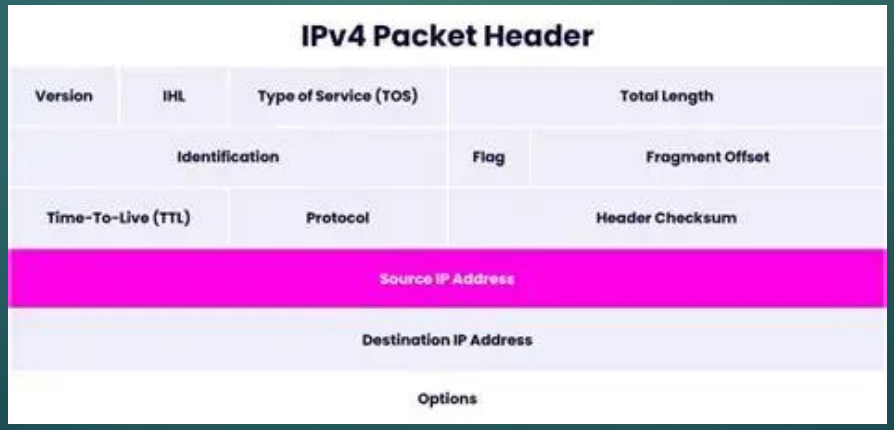
- IPv4 and IPv6 are the core protocols that move data across networks.
- Attackers often target weaknesses at this foundational layer.
- Understanding how packets work helps defend against attacks.

IPv4 Overview

- Uses 32-bit addresses (example: 192.168.1.1).
- Limited to about 4.3 billion addresses.
- Still widely used on most networks today.
- Relies heavily on NAT to conserve addresses.

IPv4 Packet Header (How an IPv4 Packet Looks)

- Version – identifies IPv4.
- Source IP Address – sender of the packet.
- Destination IP Address – receiver of the packet.
- TTL (Time to Live) – prevents infinite looping.
- Protocol – identifies TCP, UDP, or ICMP.
- Header Checksum – checks for errors.



IPv4 Security Weaknesses

- No built-in authentication.
- Susceptible to IP spoofing.
- Broadcast traffic increases attack surface.
- NAT can hide malicious activity.

IPv4 Real-Life Scenario

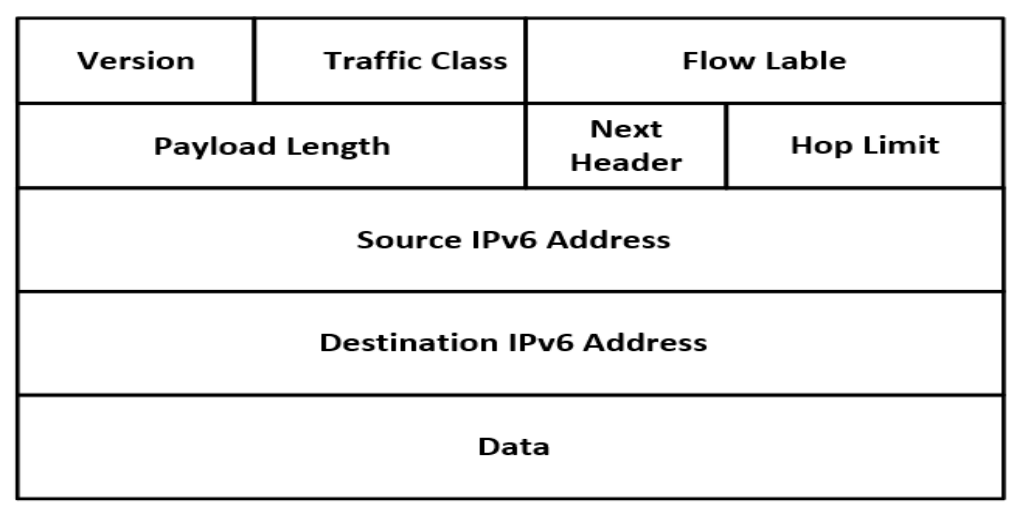
- An attacker spoofs an internal IPv4 address.
- Security systems trust the spoofed address.
- Unauthorized access is granted.
- Shows how attackers exploit IPv4 weaknesses.

IPv6 Overview

- Uses 128-bit addresses (example: 2001:db8::1).
- Provides nearly unlimited address space.
- Eliminates need for NAT.
- Designed with security improvements.

IPv6 Packet Header (How an IPv6 Packet Looks)

- Version – identifies IPv6.
- Source IPv6 Address.
- Destination IPv6 Address.
- Next Header – identifies protocol type.
- Hop Limit – prevents looping.
- Simplified header for faster routing.



IPv6 Security Strengths & Weaknesses

- Built-in support for IPsec.
- No broadcast traffic.
- Larger address space reduces scanning attacks.
- Misconfiguration introduces vulnerabilities.

IPv6 Real-Life Scenario

- Organization enables IPv6 without proper security.
- Attackers send rogue Router Advertisements.
- Traffic is redirected through attacker devices.
- Demonstrates misconfiguration risks.

IPv4 vs IPv6 Comparison

Feature	IPv4	IPv6
Address size	32-bit	128-bit
NAT	Required	Not needed
Security	Optional (Ipsec)	Built-in
Broadcast	Yes	No (uses multicast)
Address Space	Limited	Virtually infinitive

IPv4 vs IPv6 in Attacks

- IPv4 attacks rely on spoofing and broadcast abuse.
- IPv6 attacks target misconfigurations.
- Dual-stack environments increase risk.
- Both require strong security controls.

Summary & Key Takeaways

- IPv4 and IPv6 are foundational to networking.
- Attackers exploit weaknesses at this layer.
- Understanding headers improves security awareness.
- Correct configuration is essential.