Module 3:Attacking the Foundation – IPv4 and IPv6

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: **KUDZAISHE MAJEZA**

Agenda

- Introduction to IPv4 & IPv6
- IPv4 Overview
- IPv6 Overview
- IPv4 Security Weaknesses
- IPv6 Security Advantages
- IPv6 Security Weaknesses
- IPv4 vs IPv6 Security Comparison
- Summary & Key Takeaways

Introduction

- IPv4 and IPv6 are the foundational addressing protocols of the internet.
- Attackers often exploit weaknesses in these protocols.
- Understanding how they work helps secure the network more effectively.
- Module focuses on IPv4 limitations, IPv6 improvements, and related security risk

IPv4 Overview

- 32-bit address format (example: 192.168.1.1)
- 4.3 billion possible addresses
- Relies heavily on NAT because addresses are limited
- Uses broadcast messaging (less secure)
- Still the most widely used protocol globally

IPv6 Overview

- 128-bit address format (example: 2001:db8::1)
- Virtually unlimited number of addresses
- Eliminates the need for NAT
- Designed with modern networks in mind
- Supports IPsec natively for secure communication

IPv4 Security Weaknesses

- No built-in authentication or encryption
- NAT can hide malicious traffic
- Vulnerable to spoofing attacks
- Broadcast traffic may leak information
- Limited address space leads to shared networks → more attack surface

IPv6 Security Strengths

- Includes mandatory IPsec support
- Uses multicast instead of broadcast
- Larger address space makes scanning extremely difficult
- Supports secure Neighbor Discovery (SEND)
- Designed to prevent many IPv4-era weaknesses

IPv6 Security Weaknesses

- Still newer → admins misconfigure dual-stack networks
- Rogue Router Advertisement (RA) attacks
- Transition technologies (6to4, Teredo, ISATAP) can be abused
- Attack tools for IPv6 are increasing (e.g., THC-IPv6 suite)

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

Why Attackers Target the Foundation

- Attacks at the IP level affect the entire network stack
- IP spoofing enables DDoS, MITM, and session hijacking
- Misconfigured IPv6 often bypasses firewalls
- Mixed IPv4/IPv6 networks double the attack surface

Conclusion

- IPv4 and IPv6 both play major roles in network operations.
- IPv6 is more secure by design but still vulnerable if misconfigured.
- Attackers target foundational protocols because they impact everything.
- Defending endpoints requires understanding both IPv4 and IPv6 security principles.