Securing IPv6

When it comes to IPv6, one of the more contentious issues is IT security. Uninformed analysts, anit-v6 pundits, and security ne're-do-wells have created a mythos that IPv6 is inherently less secure than IPv4. The facts are that IPv6 is no less, or more, secure than its predecessor. It is a well known fact that most security breaches are a result of poor configuration management, insider hacks, or inadequate user training on security protocols. For IPv6 security, it is all about the implementation.

What Students Will Learn:

Students of the Securing IPv6 course are introduced to IPv6, threats specific to IPv6-enabled environments and the mitigation strategies, best practices for deploying IPv6 in a secure manner, and how the tools, processes, and methodologies available today can help IPv6 integrators minimize risk.

The 4-day course is designed to be a standalone course for IT staffers who have a responsibility for developing, implementing, and maintaining the security infrastructure and policies in their IT environment. Securing IPv6 covers IPv6 fundamentals, changes to many of the standard IT infrastructure components for IPv6, and the specific security issues surrounding each of these infrastructure categories. Also addressed are the impacts to security from the use of various IPv6 transition mechanisms and how to secure networks when they are in use.

Who Should Attend:

- IT security architects
- IT security engineers
- Network & System engineers
- Network operations staff
- IT staff

Course Structure:

Approximately 14 hours of lecture content
Approximately 14 hours of lab content

Max student population is 20 attendees.

Course is delivered onsite using a rolling, mobile lab.

nephos6

Course Outline

IPv6 and Security Basics

1. IPv6 Overview

- 1.1. IPv6 Technology Overview
- 1.2. IPv6 Myths
- 1.3. Adoption Drivers
  - 1.3.1. Business
  - 1.3.2. Information Technology
  - 1.3.3. Technology
- 1.4. Market Overview

2. General Security Review

- 2.1. Security Taxonomy - IPv4 vs. IPv6
- 2.2. IPsec: Myths vs Reality
- 2.3. Man-in-the-Middle (MITM)
- 2.4. Denial-of-Service (DOS)
- 2.5. Application Layer Threats
- 2.6. Phishing
- 2.7. Viruses and Worms
- 2.8. Common Security Tools and Practices
  - 2.8.1. Routers
  - 2.8.2. Firewalls (Network & Host)
  - 2.8.3. IDS/IPS/DPI
  - 2.8.4. Antivirus/Malware
  - 2.8.5. Certification/Identity Management Services

3. IPv6 Address Structure

- 3.1. Address Structure Overview
- 3.2. Address Types
- 3.3. IPv6 Address Scoping
- 3.4. Interface Identifier (IID)
  - 3.4.1. Constructing the Interface ID
  - 3.4.2. IID Alternatives (random, EUI, CGA, manual)
- 3.5. Global Address Management Policies

4. Addressing Space Threats & Mitigation

- 4.1. Public Network Information
- 4.2. Point-to-Point Ping Pong
- 4.3. Scanning Issues for Large Addressing Space
- 4.4. Using Limited-Scope Addressing
- 4.5. Using Privacy Addressing
- 4.6. Living in a NAT-Free Environment
  - 4.6.1. Using Proxies

5. IPv6 Header Formats

2.1. Nomenclature
2.2. IPv4/IPv6 Packet Structure Comparison
2.3. Packet Header
2.4. Extension header
  5.1.1. Descriptions
  5.1.2. Chaining
  5.1.3. Processing

Hands-on Lab: IPv6 on Windows 7

6. Extension Headers Threats & Mitigation

6.1. Header Length
6.2. Chain Length
6.3. Header Data
6.4. Header Types

Security Demo: Examining Extension Header Threats

7. ICMPv6

7.1. ICMPv6 overview
  7.1.1. Compare and contrast ICMP/ICMPv6
7.2. Neighbor Discovery (ND)
7.3. Comparison between ARP and The Neighbor Discovery Process
7.4. Supported ND Features
  7.4.1. SeND
7.5. Stateless Address AutoConfiguration (SLAAC)
  7.5.1. Renumbering
7.6. IPv6 Fragmentation
7.7. Path MTU Discovery
  7.7.1. Host MTU Management
  7.7.2. Operational Consideration

Hands-on Lab: IPv6 Host Discovery

Hands-on Lab: Introduction to IPv6 ACLs

Hands-on Lab: Implementing IOS Firewall

Security Demo: Living NAT Free - Compare v4 w/ NAT vs. v6 w/ property security perimeter

8. ICMPv6 Threats & Mitigation

- 8.1. Filtering Assumptions
  - 8.1.1. ICMPv6 Blocking
- 8.2. Neighbor Discovery
- 8.3. NA Spoofing
- 8.4. RA Spoofing
- 8.5. SEND
- 8.6. RA Guard
- 8.7. System Resource Protection
  - 8.7.1. Cache Management
  - 8.7.2. Timers
  - 8.7.3. Control Plane Policing (CoPP)
- 8.8. PMTU Considerations
  - 8.8.1. Fragmentation Related Issues, Blackholing

Hands-on Lab: Investigating ND & SLAAC

Hands-on Lab: ICMPv6 Filtering

Hands-on Lab: Rogue Router Advertisements

Hands-on Lab: System Parameter Tuning

9. DHCPv6

- 9.1. Compare/Contrast with DHCP
- 9.2. The DHCPv6 process
- 9.3. Stateful Autoconfiguration
- 9.4. Stateless DHCPv6 (aka DHCP-Lite)
- 9.5. DHCPv6 Prefix Delegation
- 9.6. Renumbering

Hands-on Lab: Deploying DHCPv6

10. DNS & IPv6

- 10.1. New record types (AAAA)
- 10.2. Forward and Reverse Zones
- 10.3. DNS Flow
- 10.4. Global DNS support
- 10.5. Dynamic Name Resolution Services

Hands-on Lab: Understanding DNS and IPv6

11. IPSec for IPv6

- 11.1. Overview
- 11.2. Implementations
- 11.3. Authentication Header
- 11.4. Encapsulating Security Payload
- 11.5. IKE & PKI

Hands-on Lab: Enabling IPsec and IKE

IPv6 Integration, Transition, and Security Topics

12. Dual Stack

- 12.1. Definition of Dual-Stack strategy, suitable environments
- 12.2. Configuration elements
- 12.3. Deployment considerations

13. Manual Tunnels

- 13.1. Manual Tunnel definition, applicability
- 13.2. Configuration elements
- 13.3. Deployment considerations

Hands-on Lab: Establishing manual tunnels

14. ISATAP

- 14.1. ISATAP definition, applicability
- 14.2. Configuration elements
- 14.3. Deployment considerations

Hands-on Lab: Enabling ISATAP

15. 6to4

- 15.1. 6to4 definition, applicability
- 15.2. Configuration elements
- 15.3. Deployment considerations

Hands-on Lab: Implementing 6to4

16. 6rd

- 16.1. 6rd defined, applicable environments
- 16.2. Configuration elements
- 16.3. Deployment considerations

17. Teredo

- 17.1. Teredo definition, applicability
- 17.2. Configuration elements
- 17.3. Deployment considerations

18. IP-HTTPS

- 18.1. IP-HTTPS definition, applicability
- 18.2. Configuration elements
- 18.3. Deployment considerations

19. Translation

- 19.1. NAT-PT
- 19.2. NAT64/DNS64
- 19.3. NAT444/CGN/LSN
- 19.4. NAT66/NPTv6
  - 19.4.1. Temporarily Disabling IPv6
  - 19.4.2. Getting Ready for IPv6 Implementation
  - 19.4.3. Methods for Disabling IPv6 on a Temporary Basis

20. Transition Mechanism-related Threats & Mitigations

- 20.1. Dual-Stack Security Issues
- 20.2. Manual Tunneling
- 20.3. ISATAP
- 20.4. 6to4
- 20.5. 6rd
- 20.6. Teredo
- 20.7. IP-HTTPS
- 20.8. Translation
  - 20.8.1. NAT-PT
  - 20.8.2. NAT64/DNS64
  - 20.8.3. NAT444/CGN/LSN
  - 20.8.4. NAT66/NPTv6
- 20.9. Controlling and disabling unauthorized IPv6 usage

Hands-on Lab: Attacking & Protecting Transition Mechanisms

Security Demo: Minimizing Teredo access in managed environments

Hands-on Lab: Disabling Automatic Tunneling

Security Best Practices for IPv6

21. Best Practices for Implementing and Securing IPv6 Networks

- 21.1. Compare and contrast IPv4 and IPv6 security
- 21.2. Overall Threat Review
- 21.3. IPv6 security policy development
- 21.4. Recommendation for a secure deployment
- 21.5. Considerations for securing non-traditional network environments (embedded/sensors)