IPv6 Security and Practices

COURSE OVERVIEW
The IPv6 Security and Practices class will provide a foundational knowledge of the underlying security risks, threats and best practices for an IPv6-enabled network. This course will review the security fundamentals required to plan for, design, integrate and even audit IPv6 integration in their current infrastructure. The student will be exposed to various security capabilities as well as interoperability mechanisms that will enable the student to ensure a smooth introduction of IPv6 into their environment.

PREREQUISITES
It is assumed that participants attending this course have a novice-to-intermediate level understanding of computer networking and security including:
- IPv4
- Routing / Switching / Firewalls / Mobile Devices
- Host-based configurations including Windows / Mac / *NIX / Mobile

Students should have fluency in basic computer functions such as web browsing, network configuration, and configuration tuning.

COURSE OBJECTIVES
Upon completion of this course, the student will be able to:
- Understand basic security concepts as it pertains to IPv6 • Understand the structure of the IPv6 Protocol
- Understand Port Probing and Operating System Security
- Understand unique IPv6 threats: ICMPv6 Protocol Threats, Denial of Services, Extension Header Threats
- Understand how "dual-stack" networks introduce additional risks into an enterprise environment
- Understand Firewalls, tunneling, and IPSEC as they related to transition technologies within IPv6 environments
- Concepts, risks, and threat within the Mobile IPv6 environments

COURSE OUTLINE
IPv6 Overview
- History
- Impacts of IPv6
- Security Overview
- General Risks/Threats
- Security Triads: CIA/AAA

Security and Cryptography

- Symmetric Key Encryption
- Asymmetric/Public Key Encryption
- Checksum and HASH Functions

IPSEC

- IPSEC Implementation
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Extended Sequence Number (ESN)
- AH and ESP
- IPSEC, IPv6, and Tunneling

Network Security in IPv6 Environments

- IPv4 Device Visibility
- IPv4/IPv6 Stacks
- Countermeasures in Dual-Stack Environments
- Firewalls and Intrusion Detection
- IPv6 and DNS

IPv6 Implementation Headaches

- Immature solutions
- Untested Code

Neighbor Discovery Protocol Issues

- DoS
- ICMPv6
- Solicitation Types
- Additional Attacks

First Hop Security

- Router Advertisement spoofing
- DNS and SEND attacks
- RA Guard
- RA & NDP
- Atomic Fragments & ICMPv6
- SEND & NDP
- IGMP Snooping
- DHCPv6 Guard
- IPv6 Destination Guard

IPv6 Esoteric Vulnerabilities

- Extension Headers
- Commonly used Extension Headers
- Risks and Threats: ACLS, Hop by Hop, DoS
- Fragmentation … is still an issue
- NDP /SEND
- Fragmentation …. Is STILL a problem

Address & Port Scanning

- Protocol specifications & RFC4846
- Defenses against scanning
- NetFlow & NDP cache to track Address scanning
- Port scanning in IPv6
- IDS/IPS able to see this type of scanning?

IPv6 & Multicast

- Directed attacks from flooding to resource starvation
- Define site boundaries
- Management of Nodes in multicast groups

6to4 DOS

- Routers must accept and decapsulate IPv4
- No guarantee of symmetric routing
- Go Native!

Transition and Tunneling issues

- IPv4 is here for the long term
- Tunneling tech necessary for flow between v4 and v6
- Transition zones used as backdoors since at LEAST 2002
- Automatic Tunnels & Filtering
- Transition and 6to4 – NO PROD!
- 6to4 DDoS

Access Control Lists

- What is it? IPv4/v6
- Filtering in IPv6
- IPv6 Extended ACLs
- RACLs (Reflexive ACLs)

IPv6 Firewall Filter Rules

- Dual Stack makes things complicated
- ICMP in dual-stack
- Filtering at perimeter
- Host-based firewalls
- Mobile operations
- RE0
- Layer3 and link-local forwarding

Host-Based Security Controls

- Dual Stack
- Malware targeting IPv6-enabled host
- Patching and filtering
- Spurious tunnels, rogue neighbors, forwarding of IPv6 packets
- Processing of ICMPv6
- Host-based firewalls are more complicated on v6-enabled systems
- Windows, Linux, BSD, and other

Mobile IPv6 AKA MIPv6

- Always on is a challenge
- Threats against devices, connection/network, MITM, Protocol level attacks
- Devices require host-based agent
- Connection Interception
- Mobile Media Security
- Man in the Middle
- Connection Interception and RFC 3775
- MIPv6 Signaling & Communication
- Spoofing
- DoS
- IPSEC with MIPv6
- Filtering: Active & ACLs
- MIPv6 Summary

IPv6 Security Summary

- Philosophy: v4 vs v6
- IPv6 Specific issues
- Short-term and long-term risks

WHY TRAIN WITH SUNSET LEARNING INSTITUTE?

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their technology Investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience
- You have the option to attend classes live with the instructor, at any of our established training facilities, or from the convenience of your home or office
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service
- You will work with a dedicated account manager to suggest the optimal learning path for you and/or your team
- An enthusiastic student services team is available to answer any questions and ensure a quality training experience

Interested in Private Group Training?
Contact Us