IPv6 Security

Course Objective:

IPv6 is becoming widely deployed. It is standard in all modern operating systems, major network equipment and applications. Even if not explicitly deployed in your organisation, your network devices and operating systems will support IPv6 and many of IPv6's transition mechanisms. So whilst you may not have implemented IPv6 in your network yet, you still need to secure your network against abuse using IPv6 protocols.

Modern network operating systems, including Windows, Linux, Unix, Mac OS and mobile operating systems (such as Android), support IPv6 and will use IPv6 in preference to IPv4. Further most have IPv6 turned on by default.

You need to ensure that your network is IPv6 secure and that you are ready for any future implementation of IPv6.

IPv6 brings many new security challenges and opportunities. New security techniques need to be understood and implemented. The transition to IPv6 from IPv4 presents particular security issues.

This course covers IPv6 security in detail. Each area is explained and practical guidance on mitigating each security threat is provided.

Prerequisites

A good knowledge of general networking concepts is assumed. Experience of IPv4 is Necessary.

Course Delivery and Duration

Delivery method can be Classroom and Online
Duration of Training: **5 Days**

Course Outline

1. **Introduction to IPv6 Security**

- Comparison of IPv6 and IPv4
- What is IPv6?
- Why is IPv6 required?
- Address Space
- IPv6 improvements over IPv4
- New features in IPv6
- The benefits of IPv6

- Motivations to implement IPv6
- IPv6 datagram header
- IPv6 extension headers
- ICMPv6
- IPv6 auto configuration (SLAAC & DHCPv6)
- IPv6 neighbor discovery
- Router discovery in IPv6
- RIPng, OSPFv3, IS-IS and ERIGP
- BGP and IPv6

2. IPv6 Security Threats

- Comparison of IPv6 with IPv4 threats
- Threats Common to IPv4 and IPv6
- IPv6 specific security threats
- IPv6 address architecture threats
- Scanning in IPv6
- IPv6 extension header threats
- IPv6 router header abuse
- IPv6 fragmentation threats
- ICMPv6 threats
- Neighbor discovery (ND) threats
- ND threat examples
- DHCPv6 threats
- IPv6 security testing tools

3. IPv6 Security Features

- Security Features in IPv6
- Privacy Addresses and Temporary Addresses
- RA-Guard
- IPv6 multicast security and MLD snooping
- Mobile IPv6 security
- DHCPv6 security and DHCPv6-Shield
- Dynamic routing security
- Cryptographically Generated Addresses (CGA)
- SEcure Neighbor Discovery (SEND)
- Certificate Path Messages
- Monitoring Neighbor Discovery (ND)
- Mitigating Router Advertisement (RA) attacks
- Securing Router Advertisements (RAs)
- Deploying and configuring RA-Guard
- Security at the Datalink (MacSec)
- IEEE 802.1X

4. IPv6 Firewall

- Configuring IPv6 firewalls

- IPv6 firewall filtering rules
- Filtering ICMPv6
- IPv6 extension headers
- Implementing IPv6 Ingress filtering
- Assigned IPv6 addresses
- Status of IPv6 firewalls and IDS
- Deploying IPv6 firewalls
- Mitigating IPv6 DDoS attacks
- Deploying IPv6 IPS

5. **IPv6 Transition Security**

- Dual stack threats and mitigation
- 6to4 threats and mitigation
- ISATAP threats and mitigation
- Teredo threats and mitigation