



IPv6 Sikkerhed – 3 dage!

IPv6 Security Course

Description:

IPv6 may still seem far away for your network. While your migration may still not be on schedule most operating systems and network devices have had IPv6 implemented and enabled by default. Some of them even ship with tunneling options enabled by default which your existing security policies may not account for.

Learning about IPv6 and IPv6 security is therefore essential to securing your network. With or without IPv6.

There are a number of factors that make IPv6 interesting from a security perspective. The first is the fact that it is a relatively new technology, thus it is more likely that the security implications of the protocol are overlooked. Another is the fact that IPv6 implementations are much less mature than their IPv4 counterparts.

Objectives

This course will provide the delegate with an in-depth knowledge about the security implications of deploying IPv6. Where it is similar to IPv4 and where the differences are. The entire training experience is enhanced through a number of exercises that gives the delegate the opportunity to verify many of the issues being explained throughout the course.

After attending this course, you will be able to:

- Understand the basics of IPv6
- Understand the basics of IPv6 Security
- Secure IPv6 networks against threats and attacks
- Analyze and react to denial-of-service (DoS) attacks
- Implement security standards and processes to protect your IPv6 network
- Create a secure IPv6 infrastructure
- Implement host features to prevent misuse of IPv6 resources and cross-contamination

Delegate requirements

All delegates must have an in-depth understanding of IPv4 and a understanding of IPv4 security issues. Also the delegate must be able to operate both Windows/Linux.

Time schedule

3 day course

Course Content

INTRODUCTION TO IPV6

- IPv6 in a nutshell
- Larger address space
- Hierarchical addressing
- Stateless and stateful address configuration
- Built-in security
- Extensibility
- New IPv6 header
- Mobility
- Large address space
- IPv6 Header Format
- IPv4 Compatibility
- IPv6 Operation
- IPv6 Addressing Architecture
- ICMPv6 and Neighbor Discovery Protocol
- Using DNS and DHCP with IPv6
- Supporting Security and Mobility with IPv6
- Routing in IPv6 Networks
- Using IPv6 services
- IPv6 operation and Architecture
- Basic transition mechanisms
- Tunneling protocols create new risks
- IPv6 autoconfiguration

INTRODUCTION TO IPSEC AND MOBILE IP

- IPv4 security issues
- Port scanning as one of the best known reconnaissance Techniques IPv6 Features and benefits
- Authentication and Confidentiality
- IPsec architecture

- Mobile IPv6
- IPv6 deployment and migration

INTRODUCTION TO IPV6 SECURITY

- IPv6 Security Essentials
- IPv6 Security Considerations and Recommendations
- IPv6 Neighbor Discovery trust models and threats
- Implementing Security for IPv6, Cisco Documentation
- Security Implication of Mixed IPv4/IPv6 Network
- IPv6 end-to-end security
- IPv6 headers
- IPv6 Extension Headers
- Fragmentation
- Routing Header
- Privacy
- Managing privacy extensions
- IPsec, VPNs, IKE, PKI
- IPv6 autoconfiguration and ICMP

IPV6 AND IPV4 THREAT COMPARISON

- Best-Practice Evaluation
- Overview of IPv4 Topology and Best-Practice Security Rules
- Threat Analysis Attacks with New Considerations in IPv6
- Reconnaissance
- Unauthorized Access
- Header Manipulation and Fragmentation
- Layer 3-Layer 4 Spoofing ARP and DHCP Attacks Broadcast Amplification Attacks
- IPv6 and IPv4 Threat Comparison
- Translation, Transition, and Tunneling Mechanisms
- Attacks with Strong IPv4 and IPv6 similarities
- Sniffing

- Application Layer Attacks
- Rogue Devices
- Man-in-the-Middle Attacks
- Flooding
- IPv6 Security Considerations
- Authorization for Automatically Assigned Addresses and Configurations
- Protection of IP Packets
- Host Protection from Scanning and Attacks
- Control of What Traffic is Exchanged with the Internet
- Reconnaissance Tools

IPv6 NETWORK VULNERABILITIES AND ATTACKS

- Detailed analysis of IPv6 headers
- Elimination of NAT
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Ethernet LAN Security
- ICMP Attacks
- IPv6 Spoofing
- Network Security at the Data Link Layer (Layer 2) of LAN
- Network Security at the Network Layer (Layer 3: IP)
- Network Security at the Transport Layer (Layer 4: TCP and UDP)

Dato: 23. – 25. november 2011

Sted: Global Knowledge, Stamholmen 149, 7., 2650 Hvidovre

Pris: Kr. 14.950,- Prisen er ekskl. moms, inkl. materialer og forplejning

Underviser: Lasse Kim Christiansen

Information & Tilmelding:

Ønsker du mere information eller at tilmelde dig kurset, kontaktes vi på telefon 4488 1800 eller email

training@globalknowledge.dk

Velkommen!