IPv6 und Security

Netze und Endgeräte richtig absichern

Die Einführung von IPv6 wirft für Provider, für Enterprise-Netzbetreiber und Privatkunden neue Security-Fragen auf. Gibt es doch mit IPv6 neue Möglichkeiten, ein Netzwerk zu kompromittieren. Zum einen sind es Abarten bereits bestehender Angriffsarten, zum anderen reißt IPv6 neue Sicherheitslücken auf. Um ein IPv6 Netzwerk zu schützen, muss neben diesen grundlegenden Sicherheitsfragen geklärt werden, ob die bislang verwendeten Komponenten wie Firewalls, Proxys oder IPS für IPv6 ausgerüstet sind. Wie wird eine Migration aus Sicht der Security richtig durchgeführt? Was ändert sich nach dem Wegfall von NAT durch die permanente Erreichbarkeit durch öffentliche Adressen? Dieser IPv6 Security Kurs gibt einen detaillierten Überblick über diese brandaktuellen Fragen. Die Teilnehmer lernen, die Gefährdungslage durch IPv6 für ihr Netzwerk einzuschätzen und eine umfassende Absicherung zu planen.

Kursinhalt

- Neue Angriffspunkte durch IPv6
- IPv6-Adressierung absichern
- Die Hilfsprotokolle ICMPv6 und DHCPv6 aus Sicherheitssicht
- IPv6 und First Hop Security
- IPv6-Netzwerke sichern
- Absicherung von Endgeräten
- Router bei IPv6 absichern
- Firewalls an IPv6 anpassen
- Die Migration absichern

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Der Kurs eignet sich für Planer, Administratoren und Security-Beauftragte, die eine Migration hin zu IPv6 planen, vorbereiten oder begleiten möchten.

Voraussetzungen

Die Teilnehmer benötigen solide Kenntnisse der herkömmlichen IP-Welt und müssen mit IPv6 gut vertraut sein. Ein vorheriger Besuch des Kurses IPv6 – Adressierung, Routing und IPv4-Interworking ist unbedingt anzuraten. Weiterhin wird vorausgesetzt, dass die Teilnehmer gängige Security-Konzepte kennen und verstehen.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**IP6S**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**2 Tage**	**€ 1.595,-**
Termine in Österreich	**2 Tage**	**€ 1.595,-**
Termine in der Schweiz	**2 Tage**	**€ 2.150,-**
Online Training	**2 Tage**	**€ 1.595,-**

Termin/Kursort — Kurssprache Deutsch

16.05.-17.05.24	Online	24.10.-25.10.24	Online
11.07.-12.07.24	München	24.10.-25.10.24	Zürich
11.07.-12.07.24	Online	21.11.-22.11.24	Düsseldorf
19.09.-20.09.24	Berlin	21.11.-22.11.24	Online
19.09.-20.09.24	Hamburg	19.12.-20.12.24	Online
19.09.-20.09.24	Online	19.12.-20.12.24	Wien
24.10.-25.10.24	Frankfurt		

Stand 27.04.2024

IPv6 und Security

Inhaltsverzeichnis

IPv6 und Security – Netze und Endgeräte richtig absichern

1 Grundlegende Sicherheitsüberlegungen
1.1 Grundsätzliche Überlegungen
1.1.1 Sicherheitsmaßnahmen
1.1.2 Personal und Dienstleister
1.2 IPv4 und IPv6 – Sicherheit im Vergleich
1.2.1 Unterschiede zwischen IPv4 und IPv6
1.3 Die aktuelle Sicherheitslage
1.3.1 Vulnerable IPv6 Stacks
1.3.2 Die Firewall
1.3.3 Intrusion Prevention System
1.4 Der IPv6-Header aus Sicherheitssicht
1.4.1 Das Flow Label – Covert Channel
1.4.2 Extension Header Parsing
1.4.3 Sicherheitsrelevanz der Erweiterungsheader
1.4.4 Die Filterung von IPv6
1.5 Die Sicherheit testen - Tools für IPv6 Vulnerability Tests
1.5.1 NMAP
1.5.2 Nessus und OpenVAS
1.5.3 Paket-Generatoren
1.5.4 Die THC Toolsammlung
1.5.5 SI6 Tools

2 IPv6-Adressierung aus Sicherheitssicht
2.1 Sicherheitsrelevanz von NAT
2.1.1 IPv6-IPv6 Network Prefix Translation (NAT66)
2.2 Sicherheitsbetrachtungen zu den Adressarten
2.2.1 EUI 64 – Großer Wiedererkennungswert
2.2.2 Temporäre Adressen
2.3 IPv6-Adressen auskundschaften
2.3.1 Passive Sniffing
2.3.2 Detect-New-IP6
2.3.3 Multicast Enumeration
2.3.4 Alive6
2.3.5 Registrierungs-Abfrage
2.3.6 IPv6 Netze scannen
2.3.7 IPv6-Adressen erraten
2.3.8 DNS Reconnaissance

3 IPv6 und First Hop Security
3.1 Neighbor-Discovery-Angriffe
3.1.1 Trust Models and Threats
3.1.2 NDP Spoofing
3.1.3 Neighbor Unreachability Detection (NUD)
3.1.4 DoS_New_IP6
3.1.5 NDP Exhaustion Attack
3.1.6 Neighbor Advertisement Flooding
3.2 SLAAC Angriffe
3.2.1 Rogue Router
3.2.2 Man in the Middle mit RAs
3.2.3 Faked Default Gateway
3.2.4 RA Flooding
3.3 DHCPv6 Angriffe
3.3.1 DHCPv6 Starvation
3.3.2 Rogue DHCPv6 Server
3.4 ICMPv6-Angriffe
3.4.1 Amplification Attack
3.4.2 Redirect-Angriffe
3.5 ACLs zur Sicherung
3.5.1 Rogue Router ausgrenzen
3.5.2 Rogue DHCP Server verhindern
3.5.3 RA Guard
3.5.4 DHCPv6 Guard/Shield
3.5.5 NDP Snooping
3.5.6 NDP Inspection
3.6 SEND
3.6.1 RAs mit SEND absichern
3.6.2 SEND und Stateful Autoconfiguration

4 Sicherheit von IPv6-Netzen
4.1 Router in IPv6 Netzwerken sichern
4.1.1 IPv6 ACLs aufsetzen
4.1.2 Eingehender Verkehr
4.1.3 Adressen Filtern
4.1.4 ICMPv6 filtern
4.1.5 Sicherung der Routingprotokolle
4.1.6 Authentisierung bei Routing Protokollen
4.1.7 BGP-4 – Verwendung von Link Local Unicasts
4.1.8 IP Spoofing verhindern
4.2 Firewalls anpassen
4.2.1 IPv6-Fähigkeit hinterfragen
4.2.2 Check Point
4.2.3 Cisco-ASA
4.2.4 Palo Alto
4.2.5 Fortinet
4.2.6 Juniper
4.2.7 Barracuda
4.2.8 Objekte anpassen
4.2.9 Regelwerke ergänzen
4.2.10 Bogon Filtering
4.3 Radius und IPv6
4.3.1 IPv6-Konnektivität herstellen
4.3.2 Freeradius und IPv6
4.3.3 Microsoft – Network Policy Server
4.3.4 RADIUS-IPv6-Attribute
4.4 IPS in IPv6-Netzen
4.5 Proxys in IPv6-Netzen
4.6 IPsec in IPv6-Netzen
4.6.1 Einsatzmöglichkeiten von IPsec
4.6.2 Host to Host Szenario
4.6.3 IPv6-VPNs
4.6.4 IPv6-VPDN mit IPsec
4.6.5 IPsec RAS VPNs und IPv6

5 Sicherheit während der Migration
5.1 Gedanklicher Umzug zu IPv6
5.2 IPv6 Latent Threats
5.3 Dual Stack – Doppelter Schutz notwendig
5.3.1 Endgerätesicherheit aus Sicht von IPv6
5.4 Nutzen von Tunneltechnologien hinterfragen
5.4.1 Die Tunnel-Sicherheit hinterfragen
5.4.2 Configured Tunnel sichern
5.4.3 Tunnel Traffic verschlüsseln

A Offline-Lab-Übungen
A.1 Lab Übungen im Kurs
A.1.1 Laboraufbau
A.2 Übungen Kapitel 2
A.3 Übungen Kapitel 3

B Online-Lab-Übungen
B.1 Lab Übungen im Kurs
B.1.1 Laboraufbau
B.2 Übungen Kapitel 2
B.3 Übungen Kapitel 3

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de