

Aufbaukurs: IPv6-Sicherheit

Hinweis zum Bestellablauf: Bitte nehmen Sie die verbindliche Bestellung über die elektronische Einkaufsplattform des Kaufhaus des Bundes (KdB) vor.
Vertrags ID: 21861-01, Kurzbezeichnung: IPv6 – Schulungen – Los 9, Lieferant: ExperTeach GmbH

Die Einführung von IPv6 wird zu neuen Möglichkeiten führen, ein Netzwerk zu kompromittieren.

Sämtliche Änderungen, die mit der Einführung von IPv6 einhergehen, werden in diesem Kurs angesprochen und sicherheitskritisch hinterfragt. Die Themen sind:

- die Adressierung, die neuen Adressarten sowie die Adresszuweisung mittels SLAAC und DHCPv6,
- das Fehlen von NAT und die damit einhergehende Verwendung globaler Adressen in internen Netzen,
- neue Angriffsvarianten in LAN-Umgebungen aber auch in gerouteten Netzen sowie mögliche Gegenmaßnahmen wie z.B. Anpassungen an bestehenden Security Devices wie Firewalls, IPS-Systemen und Proxys,
- Verhinderung von unbeabsichtigten Sicherheitslücken bei der Einführung von IPv6.

Die einzelnen Schulungsthemen werden durch praktische Laborübungen sowie Demonstrationen durch den Trainer verfestigt. Darüber hinaus werden zu jedem einzelnen Themengebiet die gängigen Sicherheitslösungen und Best Practices vorgestellt.

Dieser IPv6 Security Kurs hilft Teilnehmenden, die Gefährdungslage durch IPv6 für ihr Netzwerk einzuschätzen und eine umfassende Absicherung zu planen.

Kursinhalt

- Grundlegende Sicherheitsüberlegungen
- IPv6-Adressierung aus Sicherheitssicht
- IPv6-LANs Angriffe und Gegenmaßnahmen
- Router in IPv6 Netzwerken sichern
- Sicherheitslösungen anpassen – Firewalls & Co.
- Sicherheit während der Migration

Zielgruppe

Dieser Aufbaukurs richtet sich an Security-Beauftragte, die eine Einführung von IPv6 in einem Netzwerk durchführen sollen und mögliche Sicherheitsprobleme bereits im Vorfeld abschätzen wollen sowie an weitere Interessierte, Netzwerker und Administratoren mit tiefen Kenntnissen der Netzwerk- und Kommunikationsinfrastrukturen.

Voraussetzungen

Die Teilnehmenden sollten über fundierte Netzwerk-Kenntnisse verfügen sowie bereits Erfahrungen mit IPv4-Netzwerken haben, insbesondere zu den Prinzipien von Adressierung und Subnetting. Zudem sind grundlegende IPv6-Netzwerk-Kenntnisse ebenfalls erforderlich.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.ch/go/I6PS

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.

Training		Preise zzgl. MwSt.	
Termine in Deutschland		2 Tage	
Online Training		2 Tage	
Termin/Kursort		Kursprache Deutsch	
16.10.-17.10.25	Frankfurt	27.11.-28.11.25	Frankfurt
16.10.-17.10.25	Online	27.11.-28.11.25	Online

Stand 05.06.2025



Inhaltsverzeichnis

Aufbaukurs: IPv6-Sicherheit

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 Die aktuelle Sicherheitslage
 - 1.2.2 Vulnerable IPv6 Stacks
- 1.3 Der IPv6-Header aus Sicherheitssicht
 - 1.3.1 Das Flow Label – Covert Channel
 - 1.3.2 Extension Header Parsing
 - 1.3.3 Sicherheitsrelevanz der Erweiterungsheader
 - 1.3.4 Die Filterung von IPv6
- 1.4 Die Sicherheit testen - Tools für IPv6 Vulnerability Tests
 - 1.4.1 IPv6 Port Scanner
 - 1.4.2 Schwachstellenscanner für IPv6
 - 1.4.3 Paket-Generatoren
 - 1.4.4 Die THC Toolsammlung

2 IPv6-Adressierung aus Sicherheitssicht

- 2.1 Sicherheitsrelevanz von NAT
 - 2.1.1 NAT-Varianten bei IPv4
 - 2.1.2 Ende zu Ende Adressierung bei IPv6
 - 2.1.3 Kein IP-Hiding
 - 2.1.4 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 und Netze auskundschaften
 - 2.3.1 Passive Sniffing
 - 2.3.2 Multicast Enumeration
 - 2.3.3 Registrierungs-Abfrage
 - 2.3.4 IPv6 Netze scannen
 - 2.3.5 IPv6-Adressen erraten
 - 2.3.6 DNS Reconnaissance

3 IPv6-LANs Angriffe und Gegenmaßnahmen

- 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 SEND und CGA
 - 3.6.2 RAs mit SEND absichern
 - 3.6.3 SEND und Stateful Autoconfiguration
- 3.7 IPv6 und First Hop Security
 - 3.7.1 MLD-Sicherheit
 - 3.7.2 IEEE 802.1X – LAN Security
 - 3.7.3 MACsec – Ebene 2-Verschlüsselung

4 Router in IPv6 Netzwerken sichern

- 4.1 IPv6 ACLs aufsetzen
 - 4.1.1 Eingehender Verkehr
 - 4.1.2 Adressen Filtern
 - 4.1.3 ICMPv6 filtern
- 4.2 Sicherung der Routingprotokolle
 - 4.2.1 Authentisierung bei Routing Protokollen
 - 4.2.2 BGP-4 – Verwendung von Link Local Unicast
 - 4.2.3 IP Spoofing verhindern
- 4.3 IPsec in IPv6-Netzen
 - 4.3.1 Einsatzmöglichkeiten von IPsec
 - 4.3.2 Host to Host Szenario
 - 4.3.3 IPv6-VPNs
 - 4.3.4 IPv6-VPDN mit IPsec
 - 4.3.5 IPsec RAS VPNs und IPv6
- 4.4 Mobile VPN
 - 4.4.1 Abläufe
 - 4.4.2 Überlegungen zur Sicherheit

5 Sicherheitslösungen anpassen – Firewalls & Co.

- 5.1 IPv6-Fähigkeit hinterfragen
- 5.2 Filterregeln in Dual Stack Netzen
 - 5.2.1 Ergänzung der Security Policy
 - 5.2.2 Objekte mit multiplen IPv6-Adressen
 - 5.2.3 Zuweisung statischer Adressen per DHCP

5.3 Next Generation Firewalls und Proxies

- 5.3.1 Probleme mit Content Filtering
- 5.3.2 Application Filtering
- 5.3.3 Identity Based Firewall - IP-Unabhängig
- 5.4 IPv6 IPS
 - 5.4.1 IP-Unabhängigkeit
 - 5.4.2 Neue Netzbasierte Regeln
- 5.5 Hersteller im Vergleich
 - 5.5.1 Check Point
 - 5.5.2 Cisco
 - 5.5.3 Palo Alto
 - 5.5.4 Fortinet
 - 5.5.5 Juniper
 - 5.5.6 Barracuda
- 5.6 Radius und IPv6
 - 5.6.1 IPv6-Konnektivität herstellen
 - 5.6.2 RADIUS-IPv6-Attribute
 - 5.6.3 Cisco ISE
 - 5.6.4 Microsoft – Network Policy Server
 - 5.6.5 Freeradius und IPv6
- 5.7 Proxys in IPv6-Netzen
 - 5.7.1 Proxy Varianten
 - 5.7.2 Adress-Umsetzung

6 Sicherheit während der Migration

- 6.1 Gedanklicher Umzug zu IPv6
- 6.2 IPv6 Latent Threats
- 6.3 Dual Stack – Doppelter Schutz notwendig
- 6.4 Endgerätesicherheit aus Sicht von IPv6
 - 6.4.1 Windows
 - 6.4.2 Linux
 - 6.4.3 MacOS
 - 6.4.4 Mobile Devices
- 6.5 Tunneltechnologien sichern
 - 6.5.1 Die Tunnel-Sicherheit hinterfragen
 - 6.5.2 Configured Tunnel sichern
 - 6.5.3 Tunnel Traffic verschlüsseln
- 6.6 Die Migration aus Sicherheitssicht
 - 6.6.1 Adressdesign für ein sicheres IPv6-Netz
 - 6.6.2 Best Practises

A Abkürzungsverzeichnis

B Index

