

Security mit 802.1X

Sicherheit für LAN und WLAN

Die Vielfalt der Geräte im Netzwerk, der Einsatz von externen Mitarbeitern und neue Ansätze wie Bring Your Own Device machen eine Überwachung des Zugriffs auf das Netz und die Ressourcen im Unternehmen immer notwendiger. Gleichzeitig soll eine hohe Flexibilität für die User und die Endgeräte erreicht werden. Eine Sicherung des Netzwerkzugriffs mit Hilfe von 802.1X gewinnt zunehmend an Bedeutung. Dieser Kurs bietet eine praxisorientierte und herstellerübergreifende Aufarbeitung des vollständigen Themas incl. aller tangierten Randbereiche wie RADIUS Server, Zertifikate & PKI sowie Domain Controller & LDAP. Mit Hilfe eines umfassenden Praxislabors werden sämtliche Schulungsinhalte mit Übungen vertieft.

Kursinhalt

- IEEE 802.1X – Das Konzept
- EAP-Protokoll und Methoden im Detail (Labs: MD5, FAST, PEAP, TLS)
- RADIUS-Protokoll und Server (Labs: Cisco ISE und MS NPS)
- 802.1X und VoIP, Windows Authentisierung, WoL, MAB, etc.
- 802.1X im WiFi (Labs: Cisco WiFi AP & Controller)
- Tipps für ein 802.1X Netzwerk: Authentication Order, Low-Impact Mode, etc.
- Schwächen von 802.1X – MACSec
- Zertifikate in einer 802.1X-Umgebung, Aufbau und Funktion einer PKI (Lab: MS Ent. CA)
- Anbindung an einen Verzeichnisdienst via LDAP (Lab: MS ADDS)
- Besonderheiten beim Active Directory (Group Scopes, Attribut-Formate, etc.)
- Clients für 802.1x (Labs: MS native & Cisco AnyConnect)
- Weiterführende Aspekte (NAC, NAP, Secure Group Tagging, etc.)

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

Dieser Kurs eignet sich für alle, die sich aus einem technischen Blickwinkel mit den Themen Authentisierung und Autorisierung im LAN und WLAN befassen wollen.

Voraussetzungen

Sie sollten Grundkenntnisse zu Ethernet und WLAN mitbringen und sich in der IP-Welt heimisch fühlen. Vertrautheit mit Microsoft-Betriebssystemen ist hilfreich, aber nicht unbedingt erforderlich.

Dieser Kurs im Web



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

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	3 Tage	CHF 2.195,-
Online Training	3 Tage	CHF 2.195,-
Termin/Kursort	Kursprache Deutsch	
09.09.-11.09.24	Düsseldorf	09.09.-11.09.24 Online

Stand 10.03.2024



EXPERTeach



Inhaltsverzeichnis

Security mit 802.1X – Sicherheit für LAN und WLAN

1 Sicherheit im LAN und WLAN	4.8 Authentisierungs-Arten	6.7.2 Unterschiedliche Forests
1.1 Klassische LAN Security	4.8.1 Computer-Authentisierung	6.8 LDAP-Autorisation
1.1.1 Device Hardening	4.8.2 Benutzer-Authentisierung	6.9 LDAP-Filter
1.1.2 Sicherung der Infrastruktur	4.8.3 Zweistufige Authentisierung	6.10 Kerberos, LDAP & RADIUS
1.2 Spoofing	4.8.4 Authentication Chaining	6.11 Checkliste
1.3 Port Security – der Klassiker	4.9 Wake on LAN und 802.1x	
1.4 DHCP Snooping	4.9.1 Preboot Execution Environment	7 802.1X in der Praxis – Übungen
1.5 Dynamic ARP Inspection	4.10 VoIP und 802.1x	7.1 Vorbereitungen
1.6 IP Source Guard	4.10.1 Phone Authentication	7.1.1 Das Testlabor
1.7 uRPF gegen IP Spoofing	4.10.2 VLAN Provisioning	7.1.2 Switch:ISE Installation
1.8 Private VLANs	4.10.3 Device Authentication	7.1.3 Switch-Grundkonfiguration
1.9 Stateless Packet Filter		7.1.4 Globale 802.1X Authentisierungs-Parameter
1.10 Port-gebundene Access-Listen	5 Public Key Infrastructure	7.1.5 802.1X Switchport-Konfiguration
1.10.1 Router Access-Listen (RACL)	5.1 Zertifikate ausstellen	7.2 Übung 1: EAP-MD5
1.10.2 VLAN Access-Lists (VACL)	5.1.1 Gültigkeits Zeitraum	7.2.1 Authenticator konfigurieren
1.11 Identity Based Network Services	5.1.2 Antragsteller	7.2.2 Benutzer anlegen
	5.1.3 Key Usage & Enhanced Key Usage	7.2.3 Authentisierung-Methode einrichten
2 IEEE 802.1X – Portbasierte Authentisierung	5.1.4 Key Store	7.2.4 AnyConnect als Supplicant
2.1 IEEE 802.1X – Das Grundkonzept	5.2 Authentifizierung	7.2.5 802.1X mit EAP-MD5 testen
2.1.1 Komponenten	5.3 Verschlüsselung	7.2.6 VLAN Provisioning
2.1.2 Protokolle	5.4 Certificate Revocation List	7.2.7 Globale Autorisierungs-Parameter
2.2 Das Extensible Authentication Protocol (EAP)	5.4.1 CRL Security	7.2.8 Autorisierung testen
2.3 EAP-Methoden	5.4.2 Laufzeit	7.2.9 Sperren des Benutzers
2.3.1 EAP-MD5 – Der Ablauf	5.4.3 Delta CRLs	7.3 Übung 2: Mac Address Bypass
2.3.2 PEAP – Der Ablauf	5.4.4 Autorisierung	7.3.1 Switch-Konfiguration
2.3.3 EAP-TLS	5.4.5 Verfügbarkeit	7.3.2 Authentication
2.3.4 EAP-FAST	5.4.6 Verfügbarkeit, ff.	7.3.3 Benutzer anlegen
2.3.5 EAP-Vergleich	5.4.7 Critical	7.3.4 Authorization
2.4 Komponenten von 802.1X	5.4.8 Sperrgrund	7.3.5 MAB testen
2.4.1 Supplicants	5.4.9 Speicherorte	7.3.6 MAC Adresse Ändern
2.4.2 Switches	5.5 Infrastruktur	7.4 Übung 3: WiFi
2.4.3 RADIUS-Server	5.5.1 Path Validation	7.4.1 Authentisierungs-Methode hinzufügen
2.5 Die Probleme	5.5.2 Path Discovery	7.4.2 WiFi Autorisierung
	5.5.3 Veröffentlichungspunkte	7.4.3 WLAN Controller Konfiguration
3 RADIUS	5.5.4 Online Certificate Status Protocol	7.4.4 Supplicant Konfiguration
3.1 RADIUS – Zentrale Zugangskontrolle	5.5.5 Lebenszyklus	7.4.5 802.1X mit EAP-FAST testen
3.1.1 RADIUS – Der Ablauf	5.6 Microsoft CA Typen	7.5 Übung 4: PEAP (MSCHAPv2)
3.1.2 RADIUS und EAP	5.7 Simple Certificate Enrollment Protocol	7.5.1 Certification Authority
3.1.3 RADIUS – Change of Authorization (CoA)	5.8 Public PKI	7.5.2 Root Zertifikat in der ISE importieren
3.1.4 RADIUS und EAP-MD5	5.9 Checkliste	7.5.3 Certificate Signing Request generieren
3.1.5 RADIUS und PEAP		7.5.4 Zertifikat beantragen
3.1.6 RADIUS und EAP-TLS	6 Verzeichnisdienste	7.5.5 Zertifikat importieren
3.1.7 RADIUS und MAC Bypass	6.1 Was ist ein Verzeichnisdienst?	7.5.6 Benutzer anlegen
3.1.8 RADIUS und Encryption Keys	6.2 Active Directory Domain Services	7.5.7 Gruppe anlegen
3.2 RADIUS Accounting	6.2.1 Domänen und Vertrauensstellungen	7.5.8 Identity Store hinzufügen
3.3 Externe Datenbanken	6.2.2 Active-Directory-Datenbank	7.5.9 Client der Domäne hinzufügen
3.4 RADIUS-Redundanz	6.2.3 Kerberos	7.5.10 Windows Supplicant konfigurieren
3.5 Network Access Control	6.2.4 Functional Level	7.5.11 802.1X mit PEAP(MS-CHAPv2) testen
3.6 Network Policy Server – Microsoft	6.2.5 Organisationseinheiten	7.5.12 Benutzer das Dial-in Recht entziehen
3.7 FreeRadius – Open Source	6.2.6 Benutzer und Computer	7.6 Übung 5: EAP-TLS
3.8 Cisco's Identity Service Engine	6.2.7 Gruppenrichtlinien	7.6.1 Network Policy Server
	6.2.8 Zuweisen von Gruppenrichtlinien	7.6.2 RADIUS Zertifikat beziehen
4 IEEE 802.1X – Advanced	6.3 Authentisierung & Autorisierung	7.6.3 RADIUS Client einrichten
4.1 MAC Address Bypass	6.4 Distinguished Names	7.6.4 Einrichten einer Gruppe
4.2 Dot1x im WLAN	6.5 LDAP-Attribute	7.6.5 Network Policies
4.2.1 WLAN Controller	6.5.1 msNPAAllowDialin	7.6.6 NPS Logging
4.2.2 IEEE 802.11i	6.5.2 userAccountControl	7.6.7 Certificate Validation
4.2.3 WLAN und RADIUS	6.5.3 Kennwörter	7.6.8 Zertifikatsvorlage erstellen
4.2.4 Gastzugänge	6.5.4 accountExpires	7.6.9 Sperrlisten konfigurieren
4.3 Multiple Hosts	6.5.5 pwdLastSet	7.6.10 Autoenrollment einrichten
4.4 IEEE 802.1x-2010 (MACsec)	6.5.6 logonHours	7.6.11 Windows Supplicant via GPO konfigurieren
4.5 VLAN-Zuweisung	6.6 Gruppen	7.6.12 802.1X mit EAP-TLS testen
4.5.1 Guest und Failure VLAN	6.6.1 Group Scope	7.6.13 Zertifikat zurückziehen
4.5.2 Critical VLAN	6.6.2 Gruppen & Backlinks	
4.6 Low-Impact Mode	6.7 DC vs. GC	
4.7 Monitor Mode	6.7.1 Attribute des GC	

