Certified Wireless Security Professional Course (CWSP)

ID CWSP **Preis** 2.390,– € (exkl. MwSt.) **Dauer** 3 Tage

Im Kurspreis sind ein Practice Test und ein Examensvoucher enthalten!

Kursüberblick

Der Certified Wireless Security Professional (CWSP) Kurs ist ein Fortgeschrittenentraining für IT-Fachkräfte, die ihr Wissen im Bereich wireless network security vertiefen möchten. Aufbauend auf den Grundlagen des wireless networking behandelt der Kurs Tools, Techniken und Best Practices zur effektiven Absicherung von Wi-Fi networks.

Die Teilnehmenden lernen u. a. wireless LAN security architecture, cryptographic protocols, authentication and access control methods, rogue detection und wireless intrusion prevention systems (WIPS). Weitere Themen sind policy and risk management sowie Fallstudien realer wireless attacks and defenses.

Nach erfolgreichem Abschluss sind die Teilnehmenden bereit für die CWSP-Zertifizierungsprüfung und können ihr Wissen zur Absicherung von enterprise wireless networks praktisch anwenden.

This intensive course covers all that is required to prepare for the CWNA Certification, including:

- 5 intensive days of hands-on training
- Official CWSP practice test questions
- Exam voucher for the CWSP Certification Exam (# PW0-206)
- Mentor support after class by our Wireless Expert team

It also ensures that students leave with real hands on skills. Hands-on exercises include the following:

- WLAN Controller Security
- Wireless Intrusion Prevention Systems (WIPS)
- WLAN infrastructure or client stations
- Using Laptop Analyzers
- Fast Secure Roaming

Zielgruppe

Netzwerkadministratoren, Wireless Engineers, Sicherheitsexperten und alle, die für die Sicherheit von wireless networks verantwortlich sind.

Empfohlenes Training für die Zertifizierung zum

Certified Wireless Security Professional (CWSP)

Voraussetzungen

Gültige CWNA-Zertifizierung oder entsprechendes Wissen.

Kursziele

During this course, you will develop skills and knowledge on the following objectives:

- WLAN Discovery Techniques
- Intrusion and Attack Techniques
- 802.11 Protocol Analysis
- Wireless Intrusion Prevention Systems (WIPS) Implementation
- Layer 2 and 3 VPNs used over 802.11 networks
- Enterprise/SMB/SOHO/Public-Network Security design models
- Managed Endpoint Security Systems802.11 Authentication and Key Management Protocols
- Enterprise/SMB/SOHO/Public-Network Security Solution Implmentation
- Building Robust Security Networks from the ground up
- Fast BSS Transition (aka. Fast/Secure Roaming) Techniques
- Thorough coverage of all 802.1X/EAP types used in WLANs
- Wireless LAN Management Systems (WNMS)
- Authentication Infrastructure Design Models
- Using Secure Applications
- 802.11 Design Architectures
- Implementing a Thorough Wireless Security Policy

Kursinhalt

The Wireless LAN Security course consists of hands on learning using the latest enterprise wireless LAN security and auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with wireless LANs today, and every class and type of WLAN security solution available on the market, from wireless intrusion prevention systems to wireless network management systems.

Students who complete the course will acquire the necessary skills for implementing and managing wireless security in the enterprise by creating layer2 and layer3 hardware and software solutions with tools from the industry leading manufacturers.

This course is excellent preparation for the challenging CWSP Certification, and includes practice exams and “Exam Cram” sessions. It is also very hands-on intensive, roughly 50% hands-on, with lots of time to get your hands on real equipment to perform actual Site Survey work.

Detaillierter Kursinhalt

Hands-On Lab Exercises:

WLAN Controller Security

- Secure access to the WLAN controller using secure management protocols
- Configuring multiple WLAN profiles, each with its own authentication and cipher suites including WPA/WPA2 Personal and Enterprise
- Configuring the WLAN controller for RADIUS connectivity and authentication
- Client station connectivity to the controller – including DHCP and browsing
- Integrated rogue device discovery

Wireless Intrusion Prevention Systems (WIPS)

- WIPS installation, licensing, adding/configuring sensors, and secure console connectivity
- Configuration according to organizational policy
- Properly classifying authorized, unauthorized, and external/interfering access points
- Identifying and mitigating rogue devices
- Identifying specific attacks against the authorized WLAN infrastructure or client stations

Using Laptop Analyzers

- Installing and configuring a WLAN discovery tool
- Installing, licensing, and configuring a laptop protocol analyzer
- Installing, licensing, and configuring a laptop spectrum analyzer
- Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool
- Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer
- Capturing and analyzing a WPA2-Personal authentication in a WLAN protocol analyzer
- Capturing and analyzing a WPA2-Enterprise authentication in a WLAN protocol analyzer
- Capturing and analyzing Hotspot authentication and data traffic in a WLAN protocol analyzer
- Capturing and analyzing Beacons, Probe Requests, Probe Responses, and Association Requests with a WLAN protocol analyzer
- Viewing a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer

Fast Secure Roaming

- Configure a WLAN infrastructure with two controllers and two APs per controller. Configure APs for specific power and channel settings
- Install and configure a RADIUS server for PEAP
- Configure both controllers and an authorized client device for PEAP authentication using the CCMP cipher suite
- Configure an 802.11 protocol analyzer to capture the BSS transition
- Perform a slow BSS transition within a controller as a baseline
- Enable FSR mechanisms within controllers and the client station
- Perform a fast BSS transition within a controller as a comparison
- Perform a slow BSS transition between controllers as a baseline
- Perform a fast BSS transition (if vendor FSR mechanisms permit) between controllers as a comparison

Course Outline

Introduction to WLAN Security Technology

- Security policy

- Security concerns
- Security auditing practices
- Application layer vulnerabilities and analysis
- Data Link layer vulnerabilities and analysis
- Physical layer vulnerabilities and analysis
- 802.11 security mechanisms
- Wi-Fi Alliance security certifications

Small Office / Home Office WLAN Security Technology and Solutions

- WLAN discovery equipment and utilities
- Legacy WLAN security methods, mechanisms, and exploits
- Appropriate SOHO security

WLAN Mobile Endpoint Security Solutions

- Personal-class mobile endpoint security
- Enterprise-class mobile endpoint security
- User-accessible and restricted endpoint policies
- VPN technology overview

Branch Office / Remote Office WLAN Security Technology and Solutions

- General vulnerabilities
- Preshared Key security with RSN cipher suites
- Passphrase vulnerabilities
- Passphrase entropy and hacking tools
- WPA/WPA2 Personal – how it works
- WPA/WPA2 Personal – configuration
- Wi-Fi Protected Setup (WPS)
- Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices

Enterprise WLAN Management and Monitoring

- Device identification and tracking
- Rogue device mitigation
- WLAN forensics
- Enterprise WIPS installation and configuration
- Distributed protocol analysis
- WNMS security features
- WLAN controller security feature sets

Enterprise WLAN Security Technology and Solutions

- Robust Security Networks (RSN)
- WPA/WPA2 Enterprise – how it works
- WPA/WPA2 Enterprise – configuration
- IEEE 802.11 Authentication and Key Management (AKM)
- 802.11 cipher suites
- Use of authentication services (RADIUS, LDAP) in WLANs
- User profile management (RBAC)
- Public Key Infrastructures (PKI) used with WLANs
- Certificate Authorities and x.509 digital certificates
- RADIUS installation and configuration
- 802.1X/EAP authentication mechanisms
- 802.1X/EAP types and differences
- 802.11 handshakes
- Fast BSS Transition (FT) technologies

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch