Training: CWNP
CWSP Certified Wireless Security Professional

TRAINING GOALS:

The Certified Wireless Security Professional (CWSP) is a WLAN subject matter expert (SME) who can assist in the creation and implementation of an organization's enforceable security policy by following applicable regulations, standards, and accepted best practices. This SME can identify and mitigate threats to a wireless network. A CWSP can effectively use appropriate tools and procedures to ensure the ongoing security of the network.

Main areas covered by CWSP:

- 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

When you pass the CWSP exam and hold a valid CWNA certification, you earn the CWSP certification and credits towards the CWNE certification should you choose to pursue it.

Each participant in an authorized CWNP CWSP training held in Compendium CE will receive a free CWSP-207 Certified Wireless Security Professional Exam voucher.

CONSPECT:

- Security Policy
  - Define WLAN security Requirements
    - Evaluate and incorporate business, technical, and applicable regulatory policies (for example, PCI-DSS, HIPAA, GDPR, etc.)
    - Involve appropriate stakeholders
    - Review client devices and applications
    - Review WLAN infrastructure devices
  - Develop WLAN security policies
    - Translate security requirements to high-level policy statements

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Write policies conforming to common practices including definitions of enforcement and constraint specifications
        - Ensure appropriate approval and support for all policies
        - Implement security policy lifecycle management
    - Ensure proper training is administered for all stakeholders related to security policies and ongoing security awareness
- Vulnerabilities, Threats, and Attacks
    - Identify potential vulnerabilities and threats to determine the impact on the WLAN and supporting systems and verify, mitigate, and remediate them
    - Use information sources to identify the latest vulnerabilities related to a WLAN including online repositories containing CVEs
    - Determine the risk and impact of identified vulnerabilities
    - Select appropriate actions to mitigate threats exposed by vulnerabilities
        - Review and adjust device configurations to ensure conformance with security policy
        - Implement appropriate code modifications, patches and upgrades
        - Quarantine unrepaired/compromised systems
        - Examine logs and network traffic where applicable
    - Describe and detect possible, common WLAN attacks including eavesdropping, man-in-the-middle, cracking, phishing, and other social engineering attacks
    - Implement penetration testing procedures to identify weaknesses in the WLAN
        - Use appropriate penetration testing processes including scope definition, information gathering, scanning, attack, and documentation procedures
        - Select and use penetration testing tools including project documentation, scanners, hardware tools, Kali Linux tools, protocol analyzers, and WLAN auditing tools (software and hardware)
    - Implement network monitoring to identify attacks and potential vulnerabilities
        - Use appropriate tools for network monitoring including centralized monitoring, distributed monitoring, and Security Information Event Management (SIEM) systems
        - Implement mobile (temporary), integrated and overlay WIDS/WIPS solutions to monitor security events
    - Describe and perform risk analysis and risk mitigation procedures
    - Asset management
    - Risk ratings
    - Loss expectancy calculations
    - Develop risk management plans for WLANs
- WLAN Security Design and Architecture
    - Select the appropriate security solution for a given implementation and ensure it is

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

installed and configured according to policy requirements

- Select and implement appropriate authentication solutions
  - WPA/WPA2-Personal (Pre-Shared Key)
  - WPA/WPA2-Enterprise
  - WPA3-SAE and 192-Bit enterprise security
  - Opportunistic Wireless Encryption (OWE)
  - Fast Initial Link Setup (FILS)
  - 1X/EAP
  - Understand the capabilities of EAP methods including EAP-TLS, EAP-TTLS, PEAP, EAP-FAST, EAP-SIM, and EAP-GTC
  - Guest access authentication
- Select and implement appropriate encryption solutions
  - Encryption methods and concepts
  - Deprecated solutions TKIP/RC4
  - CCMP/AES
  - SAE and 192-bit security
  - OWE
  - Virtual Private Network (VPN)
- Select and implement wireless monitoring solutions
  - Wireless Intrusion Prevention System (WIPS) - overlay and integrated
  - Laptop-based monitoring with protocol and spectrum analyzers
- Understand and explain 802.11 Authentication and Key Management (AKM) components and processes
  - Encryption keys and key hierarchies
  - Handshakes and exchanges (4-way, SAE, OWE)
  - Pre-shared keys
  - Pre-RSNA security (WEP and 802.11 Shared Key authentication)
  - TSN security
  - RSN security
  - WPA, WPA2, and WPA3
- Implement or recommend appropriate wired security configurations to support the WLAN
  - Physical port security in Ethernet switches
  - Network segmentation, VLANs, and layered security solutions
  - Tunneling protocols and connections
  - Access Control Lists (ACLs)
  - Firewalls
- Implement authentication and security services

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Role-Based Access Control (RBAC)
- Certificate Authorities (CAs) and Public Key Infrastructure (PKI)
- AAA Servers
- Client onboarding
- Network Access Control (NAC)
- BYOD and MDM

- Implement secure transitioning (roaming) solutions
  - 11r Fast BSS Transition (FT)
  - Opportunistic Key Caching (OKC)
  - Pre-Shared Key (PSK) - standard and per-user
- Secure public access and/or open networks
  - Guest access
  - Peer-to-peer connectivity
  - Captive portals
  - Hotspot 2.0/Wi-Fi Certified Passpoint
  - OWE
- Implement preventative measures required for common vulnerabilities associated with wireless infrastructure devices and avoid weak security solutions
- 6.1 Weak/default passwords
  - Misconfiguration
  - Firmware/software updates
  - HTTP-based administration interface access
  - Telnet-based administration interface access
  - Older SNMP protocols such as SNMPv1 and SNMPv2

- Security Lifecycle Management
  - Understand and implement management within the security lifecycle of identify, assess, protect, and monitor
    - Identify technologies being introduced to the WLAN
    - Assess security requirements for new technologies
    - Implement appropriate protective measures for new technologies and validate the security of the measures
    - Monitor and audit the new technologies for security compliance (Security Information Event Management (SIEM), portable audits, infrastructure-based audits, WIPS/WIDS)
  - Use effective change management procedures including documentation, approval, and notifications
  - Use information from monitoring solutions for load observation and forecasting of future requirements to comply with security policy

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Implement appropriate maintenance procedures including license management, software/code upgrades, and configuration management
- Implement effective auditing procedures to perform audits, analyze results, and generate reports
    - User interviews
    - Vulnerability scans
    - Reviewing access controls
    - Penetration testing
    - System log analysis
    - Report findings to management and support professionals as appropriate

REQUIREMENTS:

Basic networking knowledge (OSI/IP). Basic network security concepts and wireless network administration CWNA or equivalent knowledge. To earn the CWSP certification, you must pass 2 exams: CWNA and CWSP.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

The CWSP certification is a professional level wireless LAN certification for the CWNP Program. To earn a CWSP certification, you must hold a current and valid CWNA credential. You must take the CWSP exam at a Pearson Vue Testing Center and pass with a 70% or higher. Instructors must pass with a 80% or higher. However you choose to prepare for the CWSP exam, you should start with the exam objectives, which cover the full list of skills tested on the exam. The CWSP certification is valid for three (3) years. To recertify, you must have a current CWNA credential and pass the current CWSP exam. By passing the CWSP exam, your CWNA certificate will be renewed for another three years.

CWSP exam is available through the Pearson VUE test centers.

Each participant in an authorized CWNP CWSP training held in Compendium CE will receive a free CWSP-207 Certified Wireless Security Professional Exam voucher.

TRAINER:

Authorized CWNP Trainer.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007