Training: CWNP
CWAP Certified Wireless Analysis Professional

TRAINING GOALS:

The Certified Wireless Analysis Professional (CWAP) is responsible for the capture and analysis of data related to Wireless LANs following troubleshooting principles and methodologies. This professional has an in-depth understanding of protocols, frame exchanges, and standards at the Physical layer and MAC sublayer. A CWAP is proficient in the use of spectrum and protocol analysis tools.

The main subject areas covered by CWAP:

- 802.11 Physical (PHY) Layer Frame Formats and Technologies
- 802.11 MAC Layer Frame Formats and Technologies
- 802.11 Operation and Frame Exchanges
- Spectrum Analysis and Troubleshooting
- Protocol Analysis and Troubleshooting Introduction

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

Each participant in an authorized CWNP CWAP training held in Compendium CE will receive a free CWAP-404 Certified Wireless Analysis Professional Exam voucher.

CONSPECT:

- Protocol Analysis
  - Capture 802.11 frames using the appropriate methods
    - Select capture devices
      - Laptop protocol analyzers
      - APs, controllers, and other management solutions
      - Specialty devices (hand-held analyzers and custom-built devices)
    - Install monitor mode drivers
    - Select capture location(s)
    - Capture sufficient data for analysis
    - Capture all channels or capture on a single channel as needed
    - Capture roaming events

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- Understand and apply the common capture configuration parameters available in protocol analysis tools
  - Save to disk
  - Packet slicing
  - Event triggers
  - Buffer options
  - Channels and channel widths
  - Capture filters
  - Channel scanning and dwell time
- Analyze 802.11 frame captures to discover problems and find solutions
  - Use appropriate display filters to view relevant frames and packets
  - Use colorization to highlight important frames and packets
  - Configure and display columns for analysis purposes
  - View frame and packet decodes while understanding the information shown and applying it to the analysis process
  - Use multiple adapters and channel aggregation to view captures from multiple channels
  - Implement protocol analyzer decryption procedures
  - View and use a capture’s statistical information for analysis
  - Use expert mode for analysis
  - View and understand peer maps as they relate to communications analysis
- Utilize additional tools that capture 802.11 frames for analysis and troubleshooting
  - WLAN scanners and discovery tools
  - Protocol capture visualization and analysis tools
  - Centralized monitoring, alerting, and forensic tools
- Ensure appropriate troubleshooting methods are used with all analysis types
  - Define the problem
  - Determine the scale of the problem
  - Identify probable causes
  - Capture and analyze the data
  - Observe the problem
  - Choose appropriate remediation steps
  - Document the problem and resolution

- Spectrum Analysis
  - Capture RF spectrum data and understand the common views available in spectrum analyzers
    - Install, configure, and use spectrum analysis software and hardware

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- Capture RF spectrum data using handheld, laptop-based, and infrastructure spectrum capture solutions
- Understand and use spectrum analyzer views
  - Real-time FFT
  - Waterfall, swept spectrogram, density, and historic views
  - Utilization and duty cycle
  - Detected devices
  - WLAN integration views
- Analyze spectrum captures to identify relevant RF information and issues
  - RF noise floor in an environment
  - Signal-to-Noise Ratio (SNR) for a given signal
  - Sources of RF interference and their locations
  - RF channel utilization
  - Non-Wi-Fi transmitters and their impact on WLAN communications
  - Overlapping and non-overlapping adjacent channel interference
  - Poor performing or faulty radios
- Analyze spectrum captures to identify various device signatures
  - Identify various 802.11 PHYs
    - DSSS
    - OFDM
    - OFDMA
    - Channel widths
    - Primary channel
  - Identify non-802.11 devices based on RF behaviors and signatures
    - Frequency hopping devices
    - IoT devices
    - Microwave ovens
    - Video devices
    - RF Jammers
    - Cordless phones
  - Use centralized spectrum analysis solutions
    - AP-based spectrum analysis
    - Sensor-based spectrum analysis

- PHY Layers and Technologies
  - Understand and describe the functions of the PHY layer and the PHY protocol data units (PPDUs)
    - DSSS (Direct Sequence Spread Spectrum)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- HR/DSSS (High Rate/Direct Sequence Spread Spectrum)
- OFDM (Orthogonal Frequency Division Multiplexing)
- ERP (Extended Rate PHY)
- HT (High Throughput)
- VHT (Very High Throughput)
- HE (High Efficiency)
    - HE SU PPDU
    - HE MU PPDU
    - HE ER SU PPDU
    - HE TB PPDU
    - HE NULL data packets
- Apply the understanding of PHY technologies, including PHY headers, preambles, training fields, frame aggregation, and data rates, to captured data
- Identify and use PHY information provided within pseudo-headers in protocol analyzers
    - Pseudo-Header formats
        - Radiotap
        - Per Packet Information (PPI)
    - Key pseudo-header content
        - Guard intervals
        - Resource units allocation
        - PPDU formats
        - Signal strength
        - Noise
        - Data rate and MCS index
        - Length information
        - Channel center frequency or received channel
        - Channel properties
    - Recognize the limits of protocol analyzers to capture PHY information including NULL data packets and PHY headers
    - Use appropriate capture devices based on proper understanding of PHY types
        - Supported PHYs
        - Supported spatial streams

- MAC Sublayer and Functions
    - Understand frame encapsulation and frame aggregation
        - Frame aggregation (A-MSDU and A-MPDU)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- Identify and use MAC information in captured data for analysis
  - Management, Control, and Data frames
  - MAC frame formats and contents
    - Frame Control field
    - To DS and From DS fields
    - Address fields
    - Frame Check Sequence (FCS) field
  - 11 Management frame formats
    - Information Elements
    - Authentication
    - Association and Reassociation
    - Beacon
    - Prove Request and Probe Response
  - Data and QoS Data frame formats
  - 11 Control frame formats
    - Acknowledgement (ACK)
    - Request to Send/Clear to Send (RTS/CTS)
    - Block Acknowledgement and related frames
    - Trigger frames
    - VHT/HE NDP announcements
    - Multiuser RTS
  - Validate BSS configuration through protocol analysis
    - Country code
    - Minimum basic rate
    - Supported rates and coding schemes
    - Beacon interval
    - WMM settings
    - RSN settings
    - HT/VHT/HE operations
    - Channel width
    - Primary channel
    - Hidden or non-broadcast SSIDs
  - Identify and analyze CRC error frames and retransmitted frames
- WLAN Medium Access
  - Understand 802.11 contention algorithms in-depth and know how they impact WLANs
    - Distributed Coordination Function (DCF)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

        - Carrier Sense (CS) and Energy Detect (ED)
        - Network Allocation Vector (NAV)
        - Contention Windows (CW) and random backoff
        - Interframe spacing
    - Enhanced Distributed Channel Access (EDCA)
        - EDCA Function (EDCAF)
        - Access Categories and Queues
        - Arbitration Interframe Space Number (AIFSN)
    - Wi-Fi Multimedia (WMM)
        - WMM parameters
        - WMM-Power Save
        - WMM-Admission Control
    - Analyze QoS configuration and operations
        - Verify QoS parameters in capture files
        - Ensure QoS is implemented end-to-end
- 802.11 Frame Exchanges
    - Capture, understand, and analyze BSS discovery and joining frame exchanges
        - BSS discovery
        - 11 Authentication and Association
        - 1X/EAP exchanges
        - Pre-Shared Key authentication
        - Four-way handshake
        - Group key exchange
        - Simultaneous Authentication of Equals (SAE)
        - Opportunistic Wireless Encryption (OWE)
        - WPA2 and WPA3
        - Fast secure roaming mechanisms
            - Fast BSS Transition (FT) roaming exchanges
            - Pre-FT roaming exchanges
        - Neighbor discovery (802.11k/v)
        - Hotspot 2.0 protocols and operations from the client access perspective
            - ANQP
            - Initial access
        - Analyze roaming behavior and resolve problems related to roaming
            - Sticky clients
            - Excessive roaming

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- Channel aggregation for roaming analysis
- Analyze data frame exchanges
  - Data frames and acknowledgement frames
  - RTS/CTS data frame exchanges
  - QoS Data frame exchanges
  - Block Acknowledgement exchanges
- Analyze MIMO and multiuser-specific transmission methods
  - MIMO
    - Transmit Beamforming (TxBF)
    - MU-MIMO
  - OFDMA
    - Scheduling and trigger frames
  - Analyze behavior and solve problems related to MAC layer operations
    - Power Save operations
    - Protection mechanisms
    - Load balancing
    - Band Steering

REQUIREMENTS:

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

Difficulty level



CERTIFICATE:

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

The CWAP certification is a professional level wireless LAN certification for the CWNP Program. To earn a CWAP certification, you must hold a current and valid CWNA credential. You must take the CWAP 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 CWAP exam, you should start with the exam objectives, which cover the full list of skills tested on the exam. The CWAP certification is valid for three (3) years. To recertify, you must have a current CWNA credential and pass the current CWAP exam. By passing the CWAP exam, your CWNA certificate will be renewed for another three years.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

CWAP exam is available through the Pearson VUE test centers.

Each participant in an authorized CWNP CWAP training held in Compendium CE will receive a free CWAP-404 Certified Wireless Analysis Professional Exam voucher.

TRAINER:

Authorized CWNP Trainer.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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