

Szkolenie: CWNP
CWAP Enterprise Wi-Fi Analysis & Troubleshooting 2.0

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	4300 PLN NETTO*	4 dni
Stacjonarne	Tablet CTAB	4700 PLN NETTO*	4 dni
Metoda dlearning	Tradycyjne	4300 PLN NETTO*	4 dni
Metoda dlearning	Tablet CTAB	4300 PLN NETTO*	4 dni

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

DOSTĘPNE TERMINY

2019-09-23 | 4 dni | Warszawa

2019-09-23 | 4 dni | Warszawa

Cel szkolenia:

Kurs **CWAP** analizy sieci bezprzewodowych oferuje praktyczną naukę z wykorzystaniem najnowszych narzędzi do analizy i diagnostyki korporacyjnych sieci bezprzewodowych.

Oferuje pogłębioną analizę funkcjonalności sieci radiowych, sposobów wykorzystania protokołu 802.11 i specyfikacji stowarzyszenia WiFi, formatu ramek radiowych 802.11 i ich struktury, metodologii diagnostyki błędów oraz analizy protokołu.

Oprócz tego kurs oferuje rozległy trening współczesnej analizy spektrum z naciskiem na zaawansowaną analizę RF, metod zbierania danych, interpretacji wykresów i prezentacji oraz w zrozumieniu zaawansowanych możliwości analizatorów spektrum.

Studenci, którzy ukończą **kurs CWAP Enterprise Wi-Fi Analysis & Troubleshooting 2.0** zdobędą umiejętności niezbędne do analizy, oceny i diagnostyki działania korporacyjnych sieci bezprzewodowych, wykorzystania sprzętu i oprogramowania wiodących producentów.

Plan szkolenia:

- Podstawy łączności radiowej
 - Grupa robocza 802.11

- Model referencyjny OSI oraz warstwy 802.11 PHY i MAC
- Podwarstwy i ramki danych
- Komponenty architektury sieci radiowych WLAN
- Organizacja przesyłania stacji
- Adresacja i działanie w sieci
- Architektura współczesnych produktów WLAN
- Formaty i technologie warstwy fizycznej (PHY) i MAC
 - Funkcje warstwy fizycznej
 - Funkcja i format preambuły
 - Nagłówek – przeznaczenie i struktura
 - Analiza problemów warstwy fizycznej PHY
 - Formaty ramki fizycznej PPDU
 - Składowe ramki MAC
 - Enkapsulacja MAC
 - Pola i podpola nagłówka MAC
 - Kontrola ramek
 - Typy i podtypy ramek i ich wykorzystanie
 - Adresacja
 - Zawartość ramki
 - Format ramek danych
 - Format ramek kontrolnych
 - Format ramek zarządzających
 - Elementy i pola informacji
- Funkcjonowanie protokołu
 - Transmisja ramek „beacon” i synchronizacja
 - Skanowanie
 - Klientka maszyna stanowa
 - Arbitracja 802.11
 - QoS
 - Kontrola dostępu
 - Sterowanie pasmem i przydziałem czasu transmisji
 - Fragmentacja
 - Potwierdzenia i potwierdzenia blokowe
 - Mechanizmy ochronne i wsteczna kompatybilność
 - Zarządzanie mocą
 - Dynamiczny przydział częstotliwości (DFS) i kontrola wypromieniowanej mocy (TPC)

- Bezpieczeństwo składowe, metody i wymiany pakietów
- Procedury roamingu
- Przyszłe rozszerzenia protokołu
- 802.11n
 - Formowanie wiązki
 - Multipleksowanie przestrzenne
 - Technologia Maximal Ratio Combining (MRC)
 - Kodowanie „Space-Time Block Coding”
 - Kanały 40 MHz
 - Agregacja ramek
 - Format HT-OFDM
 - Modulacja i schematy kodowania (MCS)
 - Formatowanie ramek HT
 - i więcej...
- Narzędzia do analizy protokołu i metodologia
 - Metodologia diagnostyki i usuwania błędów
 - Typy analizatorów protokołu
 - Wybór karty NIC/adaptera do analizy
 - Interpretacja wyników w oparciu o lokalizację
 - Ustawienia i możliwości analizatora
 - Filtracja i skanowanie kanałów
 - Interpretacja zdekodowanych danych
 - Wykorzystanie zaawansowanych mechanizmów analizy
 - Ocena stanu sieci WLAN i jej działania
 - Analiza i ocena statystyk sieciowych
 - Diagnostyka i usuwanie najczęstszych problemów
 - Analiza przewodowa, jako narzędzie wspomagające analizę bezprzewodową
- Narzędzia do analizy spektrum i metodologia
 - Przegląd zachowania się częstotliwości radiowych
 - Wizualizacja domen RF z wykorzystaniem narzędzi do analizy spektrum
 - Typy analizatorów spektrum i ich wykorzystanie
 - Specyfikacja i charakterystyki analizatora
 - Interpretacja prezentacji danych spektralnych
 - Interpretacja wykresów i prezentacji
 - Popularne cechy analizatorów widma WLAN
 - Identyfikacja transmitowanych wzorców

- Klasyfikacja urządzeń i ich wpływ na sieć
- Rozpoznawanie transmitowanych sygnatur

Warsztaty

- Konfiguracja analizatora protokołu, wykorzystanie i dogłębna analiza

Wykorzystanie analizatorów protokołu sieci WLAN jest podstawowym sposobem diagnostyki problemów działania sieci. W tym kursie analiza protokołu jest podstawą do ćwiczeń, a studenci będą się zapoznawać z tymi narzędziami, formatami ramek oraz działaniem protokołu. Prezentowany zestaw 10 ćwiczeń skupia się na zapoznaniu się z narzędziami do analizy protokołu, wykorzystanie ich do zbierania pakietów i interpretacji poszczególnych ramek:

- Podstawowa instalacja, zapoznanie się z możliwościami, konfiguracją i sposobem prezentacji danych
 - Otwierania, kolekcjonowanie, zachowywanie i modyfikacja plików z ramkami
 - Przegląd popularnych możliwości takich jak nazywanie urządzeń i priorytetyzacji, filtracji ruchu oraz kolorowania ramek do ułatwienia analizy
 - Konfiguracja narzędzia w celu zbierania próbki pakietów spełniających zadane kryteria
 - Identyfikacja ważnych zachowań sieci, metryk i statystyk do identyfikacji i izolacji problemów sieciowych
 - Wykorzystanie narzędzi eksperckich analizatora takich jak „conversation analysis”
 - Zdalne zbieranie ramek za pomocą punktu dostępowego AP
- Zrozumienie składowych ramki

Zestaw 9 ćwiczeń koncentruje się na wykorzystaniu narzędzi do zbierania i wizualizacji ramek 802.11, ich typów, przeznaczenia i formatów. Znajomość struktury ramek i ich zawartości jest istotna w rzeczywistej diagnostyce problemów. Zestaw ćwiczeń został tak przygotowany, aby zapoznać się z normalnymi i problematycznymi zachowaniami sieci. Nacisk został położony na:

- Zrozumienie nagłówka MAC
 - Porównanie trzech najważniejszych typów ramek i ich podtypów
 - Analiza formatów ramek poszczególnych typów
 - Analiza składowych ramek 802.11n
 - Zidentyfikowanie dodatkowych informacji raportowanych przez analizatory protokołu
 - Zrozumienie jak informacja nie jest widoczna dla analizatorów protokołu
- Wymiana ramek

Oprócz znajomości tyłów i formatów ramek w sieciach WLAN ważne jest zrozumienie jak i kiedy wykorzystywana jest dana ramka w wzajemnej komunikacji. Zrozumienie reguł wymiany ramek i zachowania sieci jest krytyczne, aby zidentyfikować jej poprawne i niepoprawne zachowanie. Niezbędne jest zrozumienie, co jest normalnym zachowaniem, aby można prawidłowo diagnozować wszelkie odchylenia. Zestaw następnego ćwiczeń koncentruje się na obserwacji i

wyjaśnieniu funkcjonowania sieci WLAN z wykorzystaniem analizatora protokołów. Następujące zagadnienia zostaną poruszone w ćwiczeniach:

- Wymiany pakietów i ich sekwencje
- Dawne i obecne mechanizmy bezpieczeństwa
- Mechanizmy ochrony ERP i HT
- Oszczędzanie mocy
- Potwierdzenia, potwierdzenia grupowe i ramki wspierające
- Dynamiczna zmiana prędkości
- Sterowanie pasmem
- i więcej...
- Diagnostyka powszechnie występujących problemów

Zestaw praktycznych ćwiczeń wystawia na próbę umiejętności diagnostyczne studentów i pozwala na podjęcie prób rozwiązania zdiagnozowanych problemów:

- Diagnostyka problemów połączeń
- Diagnostyka sekwencji 802.1X i EAP
- Diagnostyka problemów roamingu
- Konfiguracja i wykorzystanie analizatora spektrum w dogłębnej analizie

Ostatnia sekcja ćwiczeń koncentruje się na zapoznaniu się i zdobyciu pewności w wykorzystaniu analizatorów spektrum. Dokładnie zapoznamy się wykresami i grafikami wykorzystywanymi do wizualizacji danych spektralnych oraz temu jak na podstawie prezentowanych danych można określić wpływ nadajnika na sieć. Następujące kroki zostaną pokazane w ćwiczeniach:

- Instalacja analizatora i zapoznanie się ze sposobem wyświetlania danych oraz nawigacją w ramach interfejsu
- Zrozumienie "perspektywy RF" widocznej w wykresach i grafach
- Wykorzystanie wbudowanych funkcji takich jak znaczniki, jak również automatycznej identyfikacji urządzeń
- Charakterystyka zachowań źródeł interferencji
- Ocena skutków źródeł interferencji
- Określenie wpływu bliskości nadajnika na interferencje i obserwowane spektrum radiowe
- Identyfikacja sygnatur powszechnie spotykanych źródeł sygnału radiowego
- Zdalna analiza spektrum za pomocą punktów dostępowych

Wymagania:

Wymagana wiedza może zostać zdobyta w czasie kursu **CWNA**. Udział w kursie CWNA nie jest obowiązkowy. Warunkiem przystąpienia do **egzaminu CWAP** jest zdanie **egzaminu CWNA**.

Poziom trudności



Certyfikaty:

Dany kurs pomaga w przygotowaniu do **egzaminu CWAP PW0-270**, który jest dostępny w **centrach egzaminacyjnych VUE** (www.vue.com/cwnp).

Egzamin CWAP jest certyfikacją na poziomie zawodowym w programie CWNP. **Certyfikat CWAP** jest przydatny w karierze zawodowej i potwierdza posiadanie umiejętności niezbędnych do zabezpieczenia korporacyjnych sieci WiFi przed hakerami, niezależnie od typu i producenta sprzętu wykorzystywanego przez daną organizację.

Egzamin jest dostępny w języku angielskim, zawiera 60 pytań wielokrotnego wyboru. Zdanie egzaminu wymaga udzielenia co najmniej 70% poprawnych odpowiedzi.

Prowadzący:

Autoryzowany trener CWNP.