Możliwość dofinansowania

Szkolenie: Jak zostać hakerem? Pierwsze kroki w etycznym hakowaniu z Kali Linux. Rozdział 2– Ataki na sieci bezprzewodowe i ich zabezpieczanie.

Numer usługi 2025/08/11/47095/2933480

5 000,00 PLN brutto
5 000,00 PLN netto
312,50 PLN brutto/h
312,50 PLN netto/h

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

316 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
29.01.2026 do 11.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa przygotowuje uczestników do bezpiecznej i świadomej pracy z sieciami bezprzewodowymi poprzez zdobycie wiedzy na temat rodzajów sieci Wi-Fi, standardów zabezpieczeń oraz najczęstszych podatności. Uczestnicy nauczą się stosować narzędzia do analizy ruchu sieciowego, testowania odporności zabezpieczeń oraz symulacji typowych ataków w sposób zgodny z zasadami etyki i obowiązującym prawem.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	28-01-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do bezpiecznej i świadomej pracy z sieciami bezprzewodowymi poprzez zdobycie wiedzy na temat rodzajów sieci Wi-Fi, standardów zabezpieczeń oraz najczęstszych podatności. Uczestnicy nauczą się stosować narzędzia do analizy ruchu sieciowego, testowania odporności zabezpieczeń oraz symulacji typowych ataków w sposób zgodny z zasadami etyki i obowiązującym prawem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wymienia opisuje rodzaje sieci bezprzewodowych oraz zasady działania protokołu Wi-Fi.	Wskazuje sieci infrastrukturalne i adhoc, opisuje ich cechy i zastosowania.	Test teoretyczny
Charakteryzuje standardy zabezpieczeń WEP, WPA, WPA2, WPA3 wraz z ich podatnościami i konsekwencjami.	Wyjaśnia różnice technologiczne i poziomy odporności poszczególnych standardów, podaje przykłady znanych luk.	Test teoretyczny
Opisuje zasady etycznego testowania bezpieczeństwa sieci, w tym wymogi prawne i proceduralne.	Wskazuje granice legalnego testowania oraz elementy zgody na przeprowadzenie testów.	Test teoretyczny
Realizuje atak typu rogue AP, evil twin oraz deauthentication w środowisku testowym, a następnie wdraża zabezpieczenia przeciwdziałające tym atakom.	Tworzy fałszywy punkt dostępu, przeprowadza atak deauth, konfiguruje zabezpieczenia	Wywiad swobodny
Sporządza raport z testów bezpieczeństwa zgodny z dobrymi praktykami i zasadami odpowiedzialnego ujawniania luk.	Sporządza raport zawierający opis testu, zastosowane metody, uzyskane wyniki oraz rekomendacje działań naprawczych.	Obserwacja w warunkach symulowanych

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa

Nazwa Podmiotu prowadzącego walidację	Design Center
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa Podmiotu certyfikującego	Design Center
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Szczegółowy harmonogram realizacji usługi zostanie dostosowany do potrzeb i możliwości uczestników a jego finalna wersja zostanie podana zgodnie z wymaganiami systemu BUR, przed rozpoczęciem realizacji usługi.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazuje nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Moduł 1: Wprowadzenie do bezpieczeństwa sieci bezprzewodowych(1h)

- Rodzaje sieci bezprzewodowych (infrastrukturalne, ad-hoc)
- Zasady działania Wi-Fi
- Wprowadzenie do etycznego testowania (etyka, zgoda, legalność)

Moduł 2: Standardy zabezpieczeń Wi-Fi – WEP, WPA, WPA2, WPA3(2h)

- Historia rozwoju protokołów zabezpieczeń
- Różnice technologiczne i poziomy odporności
- Znane podatności i ich konsekwencje

Moduł 3: Przechwytywanie danych i analiza ruchu(3h)

- Skanowanie sieci i identyfikacja celów (airodump-ng, Kismet)
- Przechwytywanie handshake'ów WPA/WPA2
- Wstęp do analizy pakietów z Wireshark

Moduł 4: Łamanie zabezpieczeń i brute-force(3h)

- Cracking haseł z aircrack-ng i słownikami
- Wykorzystanie handshake do deszyfrowania
- Analiza skuteczności metod ataku

Moduł 5: Ataki typu rogue AP, evil twin, deauthentication(3h)

- Tworzenie fałszywego Access Pointa
- Ataki deauth (aireplay-ng)
- Symulacja przejęcia połączenia (man-in-the-middle)
- Praktyka wykrywania i przeciwdziałania

Moduł 6: Ochrona sieci i dobre praktyki(2h)

- Szyfrowanie, filtrowanie, ukrywanie SSID
- Monitorowanie środowiska sieciowego
- Dobre praktyki w zabezpieczaniu sieci domowej i firmowej

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Moduł 1: Wprowadzenie do bezpieczeństwa sieci bezprzewodowych	Paweł Pudo	29-01-2026	17:00	17:45	00:45
2 z 10 Moduł 2: Standardy zabezpieczeń Wi-Fi – WEP, WPA, WPA2, WPA3	Paweł Pudo	29-01-2026	17:45	19:15	01:30
3 z 10 Moduł 3: Przechwytywanie danych i analiza ruchu	Paweł Pudo	03-02-2026	17:00	19:15	02:15
4 z 10 Przerwa	Paweł Pudo	03-02-2026	19:15	19:30	00:15
5 z 10 Moduł 4: Łamanie zabezpieczeń i brute-force	Paweł Pudo	03-02-2026	19:30	21:00	01:30
6 z 10 cd. Moduł 4: Łamanie zabezpieczeń i brute-force	Paweł Pudo	05-02-2026	17:00	17:45	00:45
7 z 10 Moduł 5: Ataki typu rogue AP, evil twin, deauthentication	Paweł Pudo	05-02-2026	17:45	20:00	02:15
8 z 10 Moduł 6: Ochrona sieci i dobre praktyki	Paweł Pudo	10-02-2026	17:00	18:30	01:30
9 z 10 przerwa	Paweł Pudo	10-02-2026	18:30	18:45	00:15
10 z 10 Walidacja	-	10-02-2026	18:45	19:30	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	312,50 PLN
Koszt osobogodziny netto	312,50 PLN
W tym koszt walidacji brutto	120,00 PLN
W tym koszt walidacji netto	120,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Pudo

Od ponad pięciu lat Paweł Pudo intensywnie rozwija kompetencje w obszarach cyberbezpieczeństwa, administracji IT oraz edukacji cyfrowej, z powodzeniem łącząc umiejętności techniczne z talentem do klarownego przekazywania wiedzy nietechnicznym odbiorcom.

Obecnie odpowiada za całość infrastruktury IT w jednostce edukacyjnej, gdzie zarządza m.in. środowiskiem sieciowym, Azure Active Directory, pakietem Office 365, drukiem 3D i administracją stron internetowych. Równocześnie prowadzi audyty zgodne z normami ISO/IEC 27001:2017-06, ISO 22301:2020-04 oraz RODO, wspierając instytucje w budowaniu bezpiecznych i zgodnych z przepisami systemów informatycznych. Ukończył kurs audytora wiodącego SZBI (ISO 27001).

Paweł od lat prowadzi szkolenia z zakresu cyberbezpieczeństwa dla szkół, samorządów i przedsiębiorstw, dzieląc się praktyczną wiedzą i doświadczeniem. Znany z wyjątkowej umiejętności tłumaczenia skomplikowanych zagadnień technicznych w prosty i przystępny sposób, co czyni go niezwykle skutecznym edukatorem i konsultantem.

W 2021 roku ukończył studia podyplomowe "Bezpieczeństwo i ochrona cyberprzestrzeni" na Uniwersytecie Ekonomicznym w Katowicach.

W ostatnim czasie intensywnie szkoli się również w zakresie zastosowań sztucznej inteligencji w edukacji i biznesie, wykorzystując AI m.in. do budowania narzędzi szkoleniowych. Regularnie występuje jako prelegent na wydarzeniach branżowych, dzieląc się wiedzą jako członek społeczności cybersec.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma skrypt, materiały dydaktyczne w formie prezentacji oraz zestaw ćwiczeń w formie cyfrowej- pdf.

Warunki uczestnictwa

Uczestnik powinien posiadać podstawową znajomość obsługi komputera, przeglądarek internetowych i podstawowych pojęć z zakresu sieci komputerowych (IP, router, Wi-Fi).

Wymagany jest własny komputer z systemem Windows, Linux lub macOS, z uprawnieniami administratora i możliwością instalacji oprogramowania, stabilne łącze internetowe oraz karta sieciowa obsługująca tryb monitorowania i iniekcji pakietów.

Niezbędna jest umiejętność korzystania z terminala/wiersza poleceń oraz gotowość do pracy w legalnym środowisku testowym zgodnie z zasadami etyki.

Informacje dodatkowe

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

Uczestnik powinien:

- Posiadać podstawową znajomość obsługi komputera, przeglądarek internetowych oraz podstawowych pojęć z zakresu sieci komputerowych (IP, router, Wi-Fi).
- Umieć korzystać z wiersza poleceń/terminala w systemie Windows, Linux lub macOS.
- Mieć własny komputer z dostępem do Internetu oraz uprawnieniami administratora umożliwiającymi instalację oprogramowania.
- Dysponować kartą sieciową obsługującą tryb monitorowania i iniekcji pakietów
- Mieć zainstalowaną przeglądarkę internetową (Firefox lub Chrome) oraz oprogramowanie do obsługi plików PDF i archiwów ZIP/RAR.

Kontakt

Ariel Banaszewski

E-mail ariel.banaszewski@adn.pl
Telefon (+48) 22 1627 981