Możliwość dofinansowania

Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo Sieci Komputerowych (testy penetracyjne)

Numer usługi 2026/07/27/148153/3712531

10 932,24 PLN brutto
8 888,00 PLN netto
455,51 PLN brutto/h
370,33 PLN netto/h
332,00 PLN cena rynkowa

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5
30 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
24:00 h
23.12.2026 do 25.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o bezpieczeństwo sieci komputerowych oraz administrację urządzeń, które się w nich znajdują, a więc: • administratorów oraz architektów i projektantów systemów komputerowych, • pracowników działów bezpieczeństwa; audytorów i pentesterów, • pracowników wsparcia technicznego i działów supportu. ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę, która chce podnosić swoje kwalifikacje i wiedzę w temacie bezpieczeństwa sieci komputerowych — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	15-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Bezpieczeństwo Sieci Komputerowych. Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.	Laboratoria przygotowane na symulowanym środowisku kształcenia.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-sieci-komputerowych-testy-penetracyjne/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

1. Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?

- metodyki i rodzaje pentestów

- OSSTMM / OWASP
- Dokumenty opisujące dobre praktyki (NIST/CIS)
- różnice pomiędzy pentestami a audytami

2. Organizacja testów penetracyjnych

- prawne aspekty prowadzenia testów penetracyjnch
- opracowanie planu testów penetracyjnych
- popularne problemy spotykane podczas testów penetracyjnych

3. Poszczególne fazy testu penetracyjnego

» Rekonesans

- pasywne metody zbierania informacji o celu
- wykorzystanie serwerów proxy
- zbieranie i analiza metadanych
- ataki typu social-engineering i APT
- profilowanie pracowników
- aktywne metody zbierania informacji o celu
- mapowanie sieci ofiary
- omijanie firewalli

» Enumeracja podatności

- rodzaje podatności (buffer overflow, format string, etc.)
- czym jest shellcode?
- mechanizmy DEP/ASLR i ich omijanie
- ROP i heap spray’ing
- dopasowywanie kodu exploita do znalezionych podatności
- rodzaje exploitów
- wyszukiwanie exploitów
- analiza przykładowego exploita
- tworzenie własnego exploita
- wybór drogi wejścia do systemu

» Atak

- przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe
- ataki w sieci LAN/WAN/Wi-Fi
- ataki na urządzenia sieciowe (routery, switche, IDS/IPS/WAF, firewalle, load balancery)
- ataki denial of service
- fuzzing
- łamanie haseł
- atak przy pomocy exploita zdalnego
- narzędzia wspomagające atak
- podniesienie uprawnień do poziomu administratora
- exploity lokalne
- łamanie hashy haseł

» Zacieranie śladów

- backdoorowanie przejętego systemu
- zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej

» Sporządzenie raportu z testu penetracyjnego

- budowa szczegółowego raportu technicznego
- raport dla zarządu

4. Metody ochrony przed atakami

- idea honeypotów
- systemy IDS/IPS
- metody hardeningu systemów Windows
- metody hardeningu systemów Linux

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?	Zajęcia	Krzysztof Nowak	23-12-2026	09:00	12:00	03:00
2 z 10 -	Przerwa	-	23-12-2026	12:00	13:00	01:00
3 z 10 Organizacja testów penetracyjnych	Zajęcia	Krzysztof Nowak	23-12-2026	13:00	17:00	04:00
4 z 10 Poszczególne fazy testu penetracyjnego	Zajęcia	Krzysztof Nowak	24-12-2026	09:00	12:00	03:00
5 z 10 -	Przerwa	-	24-12-2026	12:00	13:00	01:00
6 z 10 Poszczególne fazy testu penetracyjnego	Zajęcia	Krzysztof Nowak	24-12-2026	13:00	17:00	04:00
7 z 10 Metody ochrony przed atakami	Zajęcia	Krzysztof Nowak	25-12-2026	09:00	12:00	03:00
8 z 10 -	Przerwa	-	25-12-2026	12:00	13:00	01:00
9 z 10 Metody ochrony przed atakami	Zajęcia	Krzysztof Nowak	25-12-2026	13:00	16:00	03:00
10 z 10 -	Walidacja	-	25-12-2026	16:00	17:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	24:00
w tym suma godzin zajęć	20:00
w tym suma godzin walidacji	01:00
w tym suma przerw	03:00
Suma godzin dydaktycznych bez przerw	28:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 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, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 932,24 PLN
Koszt przypadający na 1 uczestnika netto	8 888,00 PLN
Koszt osobogodziny brutto	455,51 PLN
Koszt osobogodziny netto	370,33 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	24:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Krzysztof Nowak

- system administrator z 17 letnim doświadczeniem
- penetration tester z 10 letnim doświadczeniem

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (zapis prezentacji).

Warunki uczestnictwa

Każdy uczestnik naszych szkoleń **musi** podpisać deklarację, że poznane ataki i narzędzia będzie wykorzystywał wyłącznie w celu testowania bezpieczeństwa swojej własnej infrastruktury i sieci .

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: co najmniej 2GB RAM, ok. 30GB HDD oraz zainstalowany darmowy i dostępny na każdy system operacyjny program VirtualBox — trener przed startem szkolenia udostępni obraz maszyny wirtualnej na której będą odbywały się laboratoria.

Informacje dodatkowe

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-sieci-komputerowych-testy-penetracyjne/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Warunki techniczne

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: co najmniej 2GB RAM, ok. 30GB HDD oraz zainstalowany darmowy i dostępny na każdy system operacyjny program VirtualBox — trener przed startem szkolenia udostępni obraz maszyny wirtualnej na której będą odbywały się laboratoria.

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl
Telefon (+48) 124 420 244