

# Usługa - Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo Sieci Komputerowych (testy penetracyjne)



0/5

## Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo Sieci Komputerowych (testy penetracyjne)

Numer usługi: 2023/01/20/148153/1666332

Dostawca usług: Niebezpiecznik.pl Piotr Konieczny

Miejsce usługi: Warszawa

Dostępność: Usługa otwarta

Forma świadczenia: stacjonarna

Status usługi: opublikowana

Identyfikator projektu: Sektor IT

PLN

3 899,00 zł netto za osobę

4 795,77 zł brutto za osobę

162,46 zł netto za osobogodzinę

199,82 zł brutto za osobogodzinę



Rodzaj  
Usługa szkoleniowa



Kategoria / Podkategoria  
Informatyka i telekomunikacja /  
Administracja IT i systemy  
komputerowe



Dofinansowanie  
Tak



od 29.03.2023  
do 31.03.2023

### Informacje o usłudze

Sposób dofinansowania:

wsparcie dla osób indywidualnych  
wsparcie dla przedsiębiorców i ich pracowników

Grupa docelowa usługi:

Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o bezpieczeństwo sieci komputerowych oraz administrację urzędów, 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:

21-03-2023

Liczba godzin usługi:

24

Podstawa uzyskania wpisu do świadczenia usługi:

Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

### Ramowy program usługi

#### 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 penetracyjnych
- 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, switchy, IDS/IPS/WAF, firewalli, 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 usługi

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?	29-03-2023	10:00	14:00	04:00
Organizacja testów penetracyjnych	29-03-2023	14:00	18:00	04:00
Poszczególne fazy testu penetracyjnego	30-03-2023	10:00	18:00	08:00
Metody ochrony przed atakami	31-03-2023	10:00	18:00	08:00

## Główny cel usługi

### Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Bezpieczeństwa 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

#### Dzięki temu szkoleniu:

poznasz techniki ataków i programy wykorzystywane przez współczesnych włamywaczy  
 dowiesz się w jaki sposób można zabezpieczyć serwery i usługi na nich pracujące przed atakami  
 nauczysz się korzystać z kilkudziesięciu narzędzi do testowania bezpieczeństwa sieci  
 własnoręcznie przeprowadzisz skuteczne ataki na usługi i urządzenia sieciowe  
 poznasz rodzaje i etapy testów penetracyjnych oraz metodyki ich prowadzenia  
 sam wykonasz test penetracyjny

Nasze szkolenie posiada unikatową formułę: **minimum teorii, maksimum praktyki**. Każde z omawianych zagadnień poprzedzamy teoretycznym wstępem oraz demonstracją odpowiednich ataków i metod ochrony w wykonaniu trenera. Główny nacisk kładziemy jednak na **ćwiczenia praktyczne** wykonywane przez uczestników.

Ćwiczeniom praktycznym poświęcamy najwięcej czasu, ponieważ to one pozwalają każdemu uczestnikowi szkolenia **własnoręcznie przeprowadzić**, a przez to **lepiej zrozumieć omawiany atak**. Podczas szkolenia do dyspozycji uczestników oddajemy sieć laboratoryjną, w której znajdują się specjalnie przygotowane serwery i usługi, wykorzystywane obecnie w realnym świecie.

Dlaczego stawiamy na praktykę? Bo sama teoria w bezpieczeństwie nie wystarcza.

powiedz mi, a zapomnę, pokaż – a zapamiętam, pozwól mi działać, a zrozumiem!

Po naszym szkoleniu będziesz naprawdę zmęczony, ale uwierz nam, że zamiast o odejściu od komputera będziesz myślał wyłącznie o tym, jak dalej pogłębiać swoją wiedzę.

## Sposób weryfikacji osiągnięcia efektów uczenia się

Test wiedzy przesyłany do Uczestników przed i po szkoleniu.

Czy usługa prowadzi do nabycia kompetencji?  Tak

---

## Kwalifikacje

Brak wyników.

---

## Cena

Koszt przypadający na 1 uczestnika netto	3 899,00 zł
Koszt przypadający na 1 uczestnika brutto	4 795,77 zł
Koszt osobogodziny netto	162,46 zł
Koszt osobogodziny brutto	199,82 zł

---

## Adres realizacji usługi

al. Aleje Jerozolimskie 123A, 02-017 Warszawa, woj. mazowieckie

Szczegóły miejsca realizacji usługi wysyłane są do Uczestników szkolenia na tydzień przed danym terminem.

## Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
  - Wi-fi
  - Lunch oraz przerwy kawowe w trakcie szkoleń stacjonarnych.
- 

## Zajęcia poprowadzą



**Krzysztof Nowak**

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

## Kontakt



**Magda Kowalska**

email: [szkolenia@niebezpiecznik.pl](mailto:szkolenia@niebezpiecznik.pl)  
tel: (+48) 124 420 244

---

## Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (podręcznik, zapis prezentacji).

2. Wieczysty dostęp do konta FTP zawierającego dodatkowe, stale aktualizowane materiały dotyczące bezpieczeństwa sieci.

### 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

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