Możliwość dofinansowania

Niebezpiecznik.pl
Piotr Konieczny

★★★★★

Szkolenie z Cyberbezpieczeństwa: Bezpieczeństwo Sieci Komputerowych (testy penetracyjne)

Numer usługi 2024/08/16/148153/2266693

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
30.12.2024 do 01.01.2025

5 533,77 PLN brutto
4 499,00 PLN netto
230,57 PLN brutto/h
187,46 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
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	20-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
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 zawiera opis efektów uczenia się?

Certyfikat zawiera opis efektów uczenia.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Certyfikat zawiera informację, że walidacja została przeprowadzona w oparciu o kryteria weryfikacji tj. laboratoria przygotowane na symulowanym środowisku kształcenia.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Certyfikat zawiera informację o zastosowaniu rozwiązań metody walidacji jaką jest obserwacja w warunkach symulowanych.

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 przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?	Krzysztof Nowak	30-12-2024	10:00	14:00	04:00
2 z 4 Organizacja testów penetracyjnych	Krzysztof Nowak	30-12-2024	14:00	18:00	04:00
3 z 4 Poszczególne fazy testu penetracyjnego	Krzysztof Nowak	31-12-2024	10:00	18:00	08:00
4 z 4 Metody ochrony przed atakami	Krzysztof Nowak	01-01-2025	10:00	18:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 533,77 PLN
Koszt przypadający na 1 uczestnika netto	4 499,00 PLN
Koszt osobogodziny brutto	230,57 PLN
Koszt osobogodziny netto	187,46 PLN

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