Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

Security/Testy Penetracyjne - wprowadzenie - forma zdalna w czasie rzeczywistym TERMIN GWARANTOWANY

Numer usługi 2024/11/08/120967/2402869

zdalna w czasie rzeczywistym
Usługa szkoleniowa
14 h
09.12.2024 do 10.12.2024

3 321,00 PLN brutto
2 700,00 PLN netto
237,21 PLN brutto/h
192,86 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest w szczególności do: administratorów systemów, administratorów bezpieczeństwa, osób wprost zajmujących się testami bezpieczeństwa - zlecających je, wykonujących lub weryfikujących ich jakość, tj. Oficerowie IT Security, Pentesterzy, Członkowie zespołów Red-Team, Blue-Team OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY: Obsługa systemów Linux, Windows na średnim poziomie, znajomość sieci oraz budowy komputera.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	02-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	14

Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do zrozumienia zależności pomiędzy podmiotami i przedmiotami bezpieczeństwa informacyjnego i cyberbezpieczeństwa. Uczestnik po szkoleniu rozróżnia metody ataków cybernetycznych, dobiera i właściwie wykorzystuje zaawansowane metody, narzędzi i technik informacyjno-komunikacyjnych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje cyberbezpieczeństwo	- definiuje cyberprzestrzeń i cyberbezpieczeństwo - charakteryzuje rodzaje testów bezpieczeństwa	Test teoretyczny
Przeprowadza testy bezpieczeństwa	- charakteryzuje strategię Red-Team - definiuje bazę testów bezpieczeństwa - charakteryzuje narzędzia przy testach bezpieczeństwa - charakteryzuje etapy wykonywania testów penetracyjnych	Test teoretyczny
Przeprowadza rraktyczne ataki w testach penetracyjnych	- definiuje Exploitation, Data Exfiltration, Lateral Movement, Persistence, Privilege Escalation	Test teoretyczny
Charakteryzuje typy ataków hackerskich	- charakteryzuje ataki komputerowe wykorzystywane przez cyberprzestępców - wyróżnia typowe błędy zabezpieczeń wykorzystywane przez atakujących - charakteryzuje ścieżkę ataku (kill-chain) - charakteryzuje ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC). - charakteryzuje ataki przez pocztę e-mail (fałszywe e-maile). - charakteryzuje ataki przez strony WWW - charakteryzuje ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam	Test teoretyczny
Stosuje dobre praktyki obrony przed atakami	- charakteryzuje dobre praktyki obrony przed atakami	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

tak

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

tak

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

tak

Program

AGENDA SZKOLENIA

1. Wstęp

- Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne, aktualne trendy na świecie.
- Rodzaje testów bezpieczeństwa.
- Analiza ryzyka w kontekście testów bezpieczeństwa.

2. Testy bezpieczeństwa.

- Strategie Red-Team oraz zespołów penetracyjnych.
- Baza testów bezpieczeństwa - projekty, standardy, wzorce.
- Narzędzia przy testach bezpieczeństwa (omówienie i prezentacja).
- Etapy wykonywania testów penetracyjnych.
- Raportowanie oraz prezentacja wyników - co zespół penetracyjny powinien. przekazywać, a czego z osoba zlecająca musi oczekiwać.

3. Praktyczne ataki w testach penetracyjnych (na bazie taktyk i technik Mitre Attack) - pokaz

i ćwiczenia:

- Exploitation
- Data Exfiltration
- Lateral Movement
- Persistence
- Privilege Escalation

4. Ogólne inne typy ataków hackerskich – prezentacja.

- Przegląd aktualnych ataków komputerowych wykorzystywanych
- przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących.
- Ścieżka ataku (kill-chain) zasady- rozpoznanie i zasady postępowania .
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC).
- Ataki przez pocztę e-mail (fałszywe e-maile).
- Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony.
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam.

5. Dobre praktyki, formy obrony przed atakami.

6. Rozwój Kompetencji z zakresu bezpieczeństwa.

Efekty uczenia zostaną zweryfikowane przed szkoleniem i po szkoleniu poprzez pre i post testy w formie testu teoretycznego zamkniętego w formie on-line.

Harmonogram

Liczba przedmiotów/zajęć: 6

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 Wstęp	Jakub Tomaszewski	09-12-2024	10:00	12:00	02:00
2 z 6 Testy bezpieczeństwa ćwiczenia	Jakub Tomaszewski	09-12-2024	12:00	14:00	02:00
3 z 6 Praktyczne ataki w testach penetracyjnych (na bazie taktyk i technik Mitre Attack) - pokaz i ćwiczenia	Jakub Tomaszewski	09-12-2024	14:00	17:00	03:00
4 z 6 Ogólne inne typy ataków hackerskich – prezentacja ćwiczenia	Jakub Tomaszewski	10-12-2024	09:00	11:00	02:00
5 z 6 Dobre praktyki, formy obrony przed atakami ćwiczenia	Jakub Tomaszewski	10-12-2024	11:00	13:00	02:00
6 z 6 Rozwój Kompetencji z zakresu bezpieczeństwa ćwiczenia	Jakub Tomaszewski	10-12-2024	13:00	16:00	03:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 321,00 PLN
Koszt przypadający na 1 uczestnika netto	2 700,00 PLN
Koszt osobogodziny brutto	237,21 PLN
Koszt osobogodziny netto	192,86 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jakub Tomaszewski

Wykształcenie: 2006 – 2007
Politechnika Poznańska, Wydział Inżynierii Elektrycznej, Informatyki, Specjalizacja: Bezpieczeństwo komputerów i sieci. Praca magisterska: "Analiza bezpieczeństwa danych w sieciach komputerowych." Stopień: Magister inżynier
2002 – 2006
Politechnika Poznańska, Wydział Inżynierii Elektrycznej, Informatyki, Specjalizacja: Systemy informacyjne, Tytuł pracy: "Paralelne pokolenie hash." Tytuł: Inżynier IT
2001 – 2002
Akademia Informatyki, nagroda dyrektorska dla najlepszego absolwenta, Specjalizacja: Projektowanie wspomagane komputerowo. Stopień: Technik IT
Specjalizacja: Bezpieczeństwo IT, Red Team Ops, Architektura bezpieczeństwa.
Doświadczenie trenerskie: Obecnie trener Altkom Akademii.
Zakres tematyczny prowadzonych szkoleń:
• IT Security
• Red Team Operation
• IT Security Architecture
• IT Security Tools
• Security Awarenes.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych, do którego składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Ogólne warunki uczestnictwa w zajęciach zostały zamieszczone na stronie:

https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

Po szkoleniu Uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Trener podczas szkolenia będzie organizował krótkie przerwy. Informacja o przerwach będzie umieszczona na slajdzie.

Warunki techniczne

Po szkoleniu uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Trener podczas szkolenia będzie organizował krótkie przerwy. Informacja o przerwach będzie umieszczona na slajdzie.

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY:

Obsługa systemów Linux, Windows na średnim poziomie, znajomość sieci oraz budowy komputera.

Kontakt

Adrianna Kukurudz

E-mail adrianna.kukurudz@altkom.pl
Telefon (+22) 801 258 566