Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

Certified Ethical Hacker - forma zdalna w czasie rzeczywistym

Numer usługi 2024/04/25/120967/2135576

zdalna w czasie rzeczywistym
Usługa szkoleniowa
58 h
29.07.2024 do 30.08.2024

4 428,00 PLN brutto
3 600,00 PLN netto
76,34 PLN brutto/h
62,07 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 do: • administratorów sieci, • osób odpowiedzialnych za infrastrukturę informatyczną, • inżynierów systemowych, • osób planujących podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji, • pracowników SOC, • administratorów witryn www, • pracowników IT planujących podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji, OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY: Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux. Zalecane przynajmniej dwuletnie doświadczenie w branży IT, znajomość protokołu TCP / IP (w tym usług takich jak DNS czy DHCP, znajomość koncepcji adresacji IP, routingu, przełączania w sieciach LAN).
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	26-07-2024

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	58
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do identyfikacji słabych punktów organizacji oraz pomaga w znalezieniu skutecznej metody obrony przed atakami na firmowe systemy. Uczestnik po szkoleniu definiuje i charakteryzuje najważniejsze techniki ataków stosowanych przez hakerów, przeprowadza rekonesans dotyczący własnej firmy czy konkurencji, skanuje, testuje i przełamuje zabezpieczenia systemów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku	- definiuje Footprinting i Rekonesans	Test teoretyczny
Analizuje podatność	- charakteryzuje narzędzia do wykonywania skanowania	Test teoretyczny
Socjotechniki (Inżynieria społeczna)	- charakteryzuje socjotechniki	Test teoretyczny
Rozpoznaje ataki na serwery webowe i aplikacje webowe	- charakteryzuje ataki na serwery webowe i aplikacje webowe	Test teoretyczny
Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing)	- charakteryzuje koncepcje i bezpieczeństwo rozwiązań chmurowych	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

tak

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa/Kategoria Podmiotu prowadzącego walidację	EC-Council
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	EC-Council
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

AGENDA SZKOLENIA

1. Wprowadzenie do „Etycznego Hakingu"
2. Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku
3. Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci
4. Enumeracja – aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze
5. Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru
6. Włamywanie się do systemów („Hakowanie” systemów)
7. Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania
8. Podsłuchiwanie (Sniffing) sieci – przechwytywanie danych
9. Socjotechniki (Inżynieria społeczna)
10. Ataki na odmowę dostępu do usługi (Denial-of-Service)
11. Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym
12. Omijanie systemów IDS, firewall’i, honeypot’ów
13. Atakowanie serwerów webowych
14. Atakowanie aplikacji webowych
15. SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL
16. Włamywanie się do sieci bezprzewodowych
17. Hakowanie platform i urządzeń mobilnych
18. Hakowanie "Internetu Rzeczy" oraz "Technologii Operacyjnych" (IoT i OT)
19. Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing)
20. Kryptografia
21. Egzamin

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY:

Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Zalecane przynajmniej dwuletnie doświadczenie w branży IT, znajomość protokołu TCP / IP (w tym usług takich jak DNS czy DHCP, znajomość koncepcji adresacji IP, routingu, przełączania w sieciach LAN).

Szkolenie liczy 58 godzin dydaktycznych (44 godziny zegarowe) łącznie z egzaminem.

Uczestnik po szkoleniu otrzymuje voucher na egzamin CEH do wykorzystania max. 30 dni po szkoleniu. Dokładny termin i godzina są ustalane indywidualnie przez Uczestnika z firmą certyfikującą dlatego termin i godziny egzaminu w harmonogramie są tylko prawdopodobne.

Egzamin online przeprowadzany jest w obecności proktora – osoby z firmy EC-Council, która podpina się zdalnie pod pulpit kursanta i obserwuje przebieg egzaminu przez kamerkę. Zdający jest zobowiązany pokazać proktorowi za pośrednictwem kamerki pomieszczenie, w którym będzie zdawał egzamin. Proktor sprawdza, czy nie ma w pokoju osób trzecich i pomocy naukowych.

METODA EGZAMINOWANIA:

Do egzaminu można przystąpić w autoryzowanych ośrodkach egzaminacyjnych EC-Council.

Format testu: Pytania wielokrotnego wyboru

Ilość pytań – 125

Czas trwania – 4 godz. zegarowe

Harmonogram

Liczba przedmiotów/zajęć: 21

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Wprowadzenie do „Etycznego Hakingu" wykład	Dominiki Węglarz	29-07-2024	10:00	11:00	01:00
2 z 21 Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku ćwiczenia	Dominiki Węglarz	29-07-2024	11:00	12:30	01:30
3 z 21 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci ćwiczenia	Dominiki Węglarz	29-07-2024	12:30	14:30	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 21 Enumeracja – aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze ćwiczenia	Dominiki Węglarz	29-07-2024	14:30	18:00	03:30
5 z 21 Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru ćwiczenia	Dominiki Węglarz	30-07-2024	09:00	12:00	03:00
6 z 21 Włamywanie się do systemów („Hakowanie” systemów) ćwiczenia	Dominiki Węglarz	30-07-2024	12:00	14:00	02:00
7 z 21 Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania ćwiczenia	Dominiki Węglarz	30-07-2024	14:00	15:00	01:00
8 z 21 Podsłuchiwanie (Sniffing) sieci – przechwytywanie danych ćwiczenia	Dominiki Węglarz	30-07-2024	15:00	17:00	02:00
9 z 21 Socjotechniki (Inżynieria społeczna) ćwiczenia	Dominiki Węglarz	31-07-2024	09:00	11:00	02:00
10 z 21 Ataki na odmowę dostępu do usługi (Denial-of-Service) ćwiczenia	Dominiki Węglarz	31-07-2024	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 21 Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym ćwiczenia	Dominiki Węglarz	31-07-2024	13:00	14:00	01:00
12 z 21 Omijanie systemów IDS, firewall'i, honeypot'ów ćwiczenia	Dominiki Węglarz	31-07-2024	14:00	17:00	03:00
13 z 21 Atakowanie serwerów webowych ćwiczenia	Dominiki Węglarz	01-08-2024	09:00	11:00	02:00
14 z 21 Atakowanie aplikacji webowych ćwiczenia	Dominiki Węglarz	01-08-2024	11:00	13:00	02:00
15 z 21 SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL ćwiczenia	Dominiki Węglarz	01-08-2024	13:00	14:00	01:00
16 z 21 Włamywanie się do sieci bezprzewodowych ćwiczenia	Dominiki Węglarz	01-08-2024	14:00	17:00	03:00
17 z 21 Hakowanie platform i urządzeń mobilnych ćwiczenia	Dominiki Węglarz	02-08-2024	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 21 Hakowanie "Internetu Rzeczy" oraz "Technologii Operacyjnych" (IoT i OT) ćwiczenia	Dominiki Węglarz	02-08-2024	11:00	13:00	02:00
19 z 21 Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing) ćwiczenia	Dominiki Węglarz	02-08-2024	13:00	14:00	01:00
20 z 21 Kryptografia ćwiczenia	Dominiki Węglarz	02-08-2024	14:00	17:00	03:00
21 z 21 Egzamin	-	12-08-2024	10:00	14:00	04:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 428,00 PLN
Koszt przypadający na 1 uczestnika netto	3 600,00 PLN
Koszt osobogodziny brutto	76,34 PLN
Koszt osobogodziny netto	62,07 PLN
W tym koszt walidacji brutto	1 230,00 PLN
W tym koszt walidacji netto	1 000,00 PLN
W tym koszt certyfikowania brutto	1,23 PLN
W tym koszt certyfikowania netto	1,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dominiki Węglarz

Wykształcenie: XIX Liceum Ogólnokształcące Profil Informatyczny w Poznaniu
Uniwersytet im. Adama Mickiewicza w Poznaniu
• Absolwent Wydziału Matematyki i Informatyki.
• Zdobył tytuł Licencjata Informatyki.
Uniwersytet im. Adama Mickiewicza w Poznaniu
• Studia uzupełniające magisterskie II-go stopnia na Wydziale Matematyki i Informatyki UAM.
Wyższa Szkoła Komunikacji i Zarządzania w Poznaniu
• Cisco Networking Academy (4 semestry Akademii Sieci Komputerowej)
Specjalizacja: Infrastruktura IT, wirtualizacja, bezpieczeństwo IT.
Doświadczenie trenerskie: Obecnie trener Altkom Akademii.
Zakres tematyczny prowadzonych szkoleń:
• VV6ICM
• VV6.5ICM
• VV6.5FT
• VV6FT
• VV6.5WN
• VV6WN
• VV6.7ICM
• VV6.7FT
• VV7ICM
• VV7FT
• BS.IT01
• BS.IT02
• CEHv9
• CEHv10
• CEHv11
• CSCU

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

Wymagania ogólne realizacji szkolenia w formule distance learning (online): Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

Adrianna Kukurudz

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