Możliwość dofinansowania

szkolenie: Bezpieczeństwo Sieci Komputerowych - testy penetracyjne

Numer usługi 2024/04/19/52766/2128776

3 813,00 PLN brutto
3 100,00 PLN netto
181,57 PLN brutto/h
147,62 PLN netto/h

NOBLEPROG POLSKA Spółka z o.o

★★★★☆

zdalna w czasie rzeczywistym
Usługa szkoleniowa
21 h
03.06.2024 do 05.06.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Uczestnikami szkolenia mogą być w szczególności pracownicy sektora IT, w szczególności menadżerowie, pracownicy odpowiedzialni za zarządzanie operacyjne, bezpieczeństwem, zarządzanie kryzysowym, ochroną zasobów, administratorzy i operatorzy systemów ochrony, administratorzy IT. Uczestnikami szkolenia mogą być również osoby, które chcą podnieść poziom swojej wiedzy, kompetencji i umiejności w zakresie cyberbezpieczeństwa, bezpieczeństwa sieci.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	30-05-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest nabycie przez uczestników wiedzy oraz umiętności w zakresie elementów systemu utrzymania bezpieczeństwa IT, a także wiedzy w zakresie prawnych aspektów zachowania cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik:		
Rozumie różnice między różnymi metodologiami testów penetracyjnych, takimi jak OSSTMM i OWASP. Wymienia dokumenty opisujące dobre praktyki, takie jak NIST czy CIS, oraz rozumie ich znaczenie dla procesu testów penetracyjnych.	Rozumie kluczowe różnice między testami penetracyjnymi a audytami, zarówno pod względem celu, jak i podejścia.	Test teoretyczny
Rozumie, jakie kwestie prawne muszą być uwzględnione podczas organizacji testów penetracyjnych.	Opisuje proces organizacji testów penetracyjnych, obejmujący zarówno techniczne jak i proceduralne aspekty.	Test teoretyczny
Rozumie wymagane aspekty prawne przeprowadzania testów penetracyjnych, takie jak zgodność z przepisami dotyczącymi prywatności i regulacjami branżowymi.	Potrafi wymienić przykłady konsekwencji naruszenia przepisów prawnych podczas testów penetracyjnych.	Test teoretyczny
Rozumie proces planowania testów penetracyjnych, obejmujący ocenę ryzyka, identyfikację celów testów i określenie zasobów potrzebnych do ich przeprowadzenia.	Opisuje elementy, które powinny być uwzględnione w planie testów penetracyjnych, takie jak harmonogram działań i cele.	Test teoretyczny
Rozumie, że podczas testów penetracyjnych mogą wystąpić różne problemy, takie jak trudności w identyfikacji podatności czy błędne interpretacje wyników testów.	Wymienia przykłady typowych problemów, takich jak konieczność dostosowania się do zmieniającego się środowiska testowego czy ograniczenia czasowe.	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, zaświadczenie z efektami uczenia się

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

Uczestnicy po szkoleniu otrzymają zaświadczenia o ukończeniu szkolenia, wraz z opisanymi efektami kształcenia.

Metodologie i typy testów penetracyjnych Standardy i wytyczne:

Wykorzystanie metodologii takich jak OSSTMM i OWASP. Wykorzystanie dokumentów opisujących dobre praktyki, takich jak NIST czy CIS. Różnice między testami penetracyjnymi a audytami:Główne różnice między testami penetracyjnymi a audytami. Organizacja testów penetracyjnych

Aspekty prawne: Wymagane aspekty prawne przeprowadzania testów penetracyjnych.

Planowanie testów penetracyjnych: Przygotowanie planu testów penetracyjnych. Typowe problemy podczas testów penetracyjnych: Typowe problemy napotykane podczas testowania. Poszczególne etapy testu penetracyjnego Rekonesans: Zbieranie informacji o celu pasywnie i aktywnie.

Analiza podatności: Identyfikacja podatności, rodzaje podatności i omijanie mechanizmów bezpieczeństwa. Atakowanie: Wykorzystywanie różnych technik ataku na systemy komputerowe i sieci.

Techniki ataków na systemy komputerowe i sieci Ataki w różnych środowiskach sieciowych: Ataki na sieci LAN/WAN/Wi-Fi i urządzenia sieciowe. Ataki typu Denial of Service: Metody przeprowadzania ataków DoS.

Narzędzia wspomagające ataki: Wykorzystanie specjalistycznych narzędzi ataków. Analiza i raportowanie Przygotowywanie raportów: Przygotowywanie raportów technicznych i raportów dla zarządu.

Ochrona przed atakami: Wykorzystanie metod ochrony, takich jak pułapki (honeypots), systemy IDS/IPS oraz metody zabezpieczania systemów Windows i Linux.

Harmonogram

Liczba przedmiotów/zajęć: 5

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 wyjkład, współdzielenie ekranu, czat Metodologie i typy testów penetracyjnych Standardy i wytyczne: Wykorzystanie metodologii takich jak OSSTMM i OWASP	DAWID KOZIOROWSKI	03-06-2024	09:00	12:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 5 wykład, ćwiczenia, Aspekty prawne	DAWID KOZIOROWSKI	03-06-2024	12:00	16:00	04:00
3 z 5 wykład, ćwiczenia, współdz.ekranu Planowanie testów penetracyjnych, Analiza podatności	DAWID KOZIOROWSKI	04-06-2024	09:00	11:00	02:00
4 z 5 wykład, wspoldz.ekranu, czat Techniki ataków na systemy komputerowe i sieci	DAWID KOZIOROWSKI	04-06-2024	11:00	16:00	05:00
5 z 5 wykład, ćwiczenia, wspoldz.ekranu Narzędzia wspomagające ataki	DAWID KOZIOROWSKI	05-06-2024	09:00	16:00	07:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 813,00 PLN
Koszt przypadający na 1 uczestnika netto	3 100,00 PLN
Koszt osobogodziny brutto	181,57 PLN
Koszt osobogodziny netto	147,62 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

DAWID KOZIOROWSKI

Wykształcenie wyższe,

Doświadczenie w prowadzeniu zajęć dydaktycznych w zakresie: bezpieczeństwo, zarządzanie kryzysowe, zarządzania ryzykiem, doświadczenie zawodowe w komórkach zarządzania kryzysowego, odbyte
szkolenia w zakresie bezpieczeństwa, audytor wiodący. Doświadczenie jako trener i szkoleniowiec 4 lata

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają dostęp do materiałów dydaktycznych online, ćwiczeń i zadań do wykonania w zakresie szkolenia.

Informacje dodatkowe

Kontakt w sprawie szkolenia, dotyczące kwestii organizacyjnych :

Monika Fengler monika.fengler@nobleprog.pl, tel. 880 997 760

Kontakt w sprawie dofinansowania do szkolenia :

Patrycja Foremniak patrycja.foremniak@nobleprog.com , tel. 694 117 999

Szkolenie zwolnione z podatku VAT w przypadku dofinansowania w wysokości 70% lub więcej. Jeśli Państwa dofinansowanie jest mniejsze niż 70% wartości netto szkolenia, prosimy o informację - do szkolenia i ceny w karcie usługi będziemy musieli doliczyć podatek VAT

Po zapisie prosimy o informację mailowo – od jakiego operatora oraz projektu otrzymali Państwo dofinansowanie oraz w jakiej wysokości.

Warunki techniczne

Wymagane:

- komputer ze stabilnym podłączeniem do Internetu (min 10Mbit/s download i 1Mbit/s upload);
- przeglądarka internetowa Chrome lub Firefox;
- dobrej jakości mikrofon lub słuchawki;
- ciche miejsce, wolne od zakłóceń i hałasu zewnętrznego

szkolenie w formie zdalnej będzie przeprowadzone na platformie do telekonferencji ZOOM .

Linki do spotkania zostaną przesłane na 2 dni przed rozpoczęciem szkolenia .

Kontakt

Patrycja Foremniak

E-mail patrycja.foremniak@nobleprog.com
Telefon (+48) 694 117 999