



Notebook Master
Sp. z o.o.



Sieci teleinformatyczne / Etap III / Bezpieczeństwo sieci - ćwiczenia praktyczne.

Numer usługi 2024/04/30/158529/2138859

📍 Bochnia / mieszana (stacjonarna połączona z usługą
zdalną w czasie rzeczywistym)

📄 Usługa szkoleniowa

🕒 24 h

📅 02.12.2024 do 04.12.2024

4 797,00 PLN brutto

3 900,00 PLN netto

199,88 PLN brutto/h

162,50 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 przedsiębiorców i ich pracowników pracujących w branży IT, którzy chcą nabyć wiedzę i umiejętności z zakresu dot. sieci teleinformatycznych, i wykorzystać je w ramach prowadzonej działalności gospodarczej i etatu.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną 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

Usługa "Sieci teleinformatyczne / Etap III / Bezpieczeństwo sieci - ćwiczenia praktyczne.", przygotowuje do samodzielnego i prawidłowego wykonywania obowiązków w zakresie dot. administrowania i konfiguracji sieci, zgodnie z planem ramowym szkolenia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Projektuje sieci wobec indywidualnych potrzeb klientów.	Prawidłowo czyta makiety szkieletowe.	Test teoretyczny
	Rozróżnia adresacje publiczną i niepubliczną zgodnie zasadami.	Test teoretyczny
Konfiguruje routing w rozbudowanych sieciach.	Rozróżnia mechanizmy translacji adresów.	Test teoretyczny
	Dobiera do sytuacji odpowiednie rodzaje routingu.	Test teoretyczny
Konfiguruje dostęp do żądanych usług w sposób bezpieczny.	Diagnostuje dostęp do konkretnych usług z poziomu konsoli.	Test teoretyczny
	Definiuje pojęcie DMZ.	Test teoretyczny
Konfiguruje firewalle dostosowane do potrzeb konkretnej sieci	Rozróżnia rodzaje firewalli.	Test teoretyczny
	Omawia budowę logiczną tabeli w firewallu.	Test teoretyczny
Zapewnia bezpieczeństwo sieciom udostępniającym usługi publicznie.	Ogranicza sfery wystąpienia ataku.	Test teoretyczny
	Monitoruje stan oprogramowania w obliczu nowych podatności.	Test teoretyczny
Zarządza ruchem w sieci.	Wymienia korzyści płynące z mądrego planowania podsieci VLAN.	Test teoretyczny
	Określa działanie VLAN.	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, dokument zawiera opis efektów uczenia się.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Szkolenie skierowane jest do przedsiębiorców i ich pracowników, chcących zwiększyć zakres własnych umiejętności. Udział w usłudze umożliwi uczestnikowi uzupełnienie i uporządkowanie dotychczasowej wiedzy z obszaru sieci teleinformatycznych.

Ramowy plan kształcenia:

I. Projektowanie sieci z uwzględnieniem:

1. Standardów bezpieczeństwa.
2. Dobrych praktyk z zakresu podziału na podsieci.
3. Współpracy z sieciami obcymi.
4. Optymalizacji ruchu sieciowego.
5. Bezpiecznego udostępniania usług w sieciach publicznych.

II. Podstawy bezpieczeństwa konfiguracji sieciowych.

1. Projektowanie ograniczenia połączeń sieciowych.
2. Analiza scenariuszy typowych ataków na sieć komputerową – faza rekonesansu.
3. Projektowanie DLP (Data Leak Prevention).
4. Projektowanie całej infrastruktury sieci wraz z systemem zabezpieczeń.
5. Analiza projektu.

III. Zaawansowane konfiguracje firewalla:

1. Firewall stateful w praktyce.
2. Budowanie reguł w oparciu o dodatkowe informacje protokołów sieciowych.
3. Analiza jakości zabezpieczeń firewall.
4. Testowanie zabezpieczeń firewall.
5. Proste użycie skanera sieciowego w diagnostyce firewall.
6. Monitoring i logowanie ruchu przy pomocy firewall.
7. Zabezpieczanie podatnych usług.
8. Gromadzenie informacji dowodowej z wykonanych połączeń.

IV. Bezpieczeństwo współpracy z sieciami podmiotów partnerskich.

1. Zagadnienia bezpieczeństwa dostępu do usług.
2. Sposoby udostępnienia usług.
3. Projektowanie i wdrażanie bezpiecznego dostępu do usług.
4. Diagnostyka zabezpieczeń.

V. Ćwiczenia praktyczne z zakresu:

1. Praktycznych scenariuszy konfiguracji sieciowych.
2. Routingu w rozbudowanych sieciach firmowych.
3. Konfigurowania bezpiecznego dostępu do usług w sieciach firmowych.
4. Konfiguracji firewalli stateless i stateful.
5. Bezpieczeństwo udostępnienia usług w sieciach publicznych.
6. Ograniczania ruchu sieciowego.

Szkolenie trwa 24 godzin dydaktycznych i realizowane jest w kameralnych grupach, maksymalnie 8-osobowych. Każdy uczestnik stacjonarny ma do dyspozycji indywidualne stanowisko szkoleniowe. Każdy uczestnik realizujący szkolenie w formie zdalnej w czasie rzeczywistym ma możliwość otrzymania od nas (za pośrednictwem kuriera) wyposażenie stanowiska szkoleniowego (po ukończeniu szkolenia sprzęt zostaje odebrany przez kuriera).

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 22 Projektowanie sieci z uwzględnieniem: Standardów bezpieczeństwa; Dobrych praktyk z zakresu podziału na podsieci; Współpracy z sieciami obcymi. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	02-12-2024	08:45	10:15	01:30	Tak
2 z 22 Przerwa.	Jacek Herold	02-12-2024	10:15	10:30	00:15	Tak
3 z 22 Projektowanie sieci z uwzględnieniem: Optymalizacji ruchu sieciowego; Bezpiecznego udostępniania usług w sieciach publicznych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	02-12-2024	10:30	12:00	01:30	Tak
4 z 22 Przerwa.	Jacek Herold	02-12-2024	12:00	12:45	00:45	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<p>5 z 22</p> <p>Podstawy bezpieczeństwa konfiguracji sieciowych: Projektowanie ograniczenia połączeń sieciowych; Analiza scenariuszy typowych ataków na sieć komputerową –faza rekonesansu. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	02-12-2024	12:45	14:15	01:30	Tak
<p>6 z 22</p> <p>Przerwa.</p>	Jacek Herold	02-12-2024	14:15	14:30	00:15	Tak
<p>7 z 22</p> <p>Podstawy bezpieczeństwa konfiguracji sieciowych: Projektowanie DLP; Projektowanie całej infrastruktury sieci wraz z systemem zabezpieczeń; Analiza projektu. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	02-12-2024	14:30	16:00	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<p>8 z 22</p> <p>Zaawansowane konfiguracje firewala: Firewall stateful w praktyce; Budowanie reguł w oparciu o dodatkowe informacje protokołów sieciowych. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	03-12-2024	08:45	10:15	01:30	Tak
<p>9 z 22</p> <p>Przerwa.</p>	Jacek Herold	03-12-2024	10:15	10:30	00:15	Tak
<p>10 z 22</p> <p>Zaawansowane konfiguracje firewala: Analiza jakości zabezpieczeń firewall; Testowanie zabezpieczeń firewall; Proste użycie skanera sieciowego w diagnostyce firewall. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	03-12-2024	10:30	12:00	01:30	Tak
<p>11 z 22</p> <p>Przerwa.</p>	Jacek Herold	03-12-2024	12:00	12:45	00:45	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<p>12 z 22</p> <p>Zaawansowane konfiguracje firewalle: Monitoring i logowanie ruchu przy pomocy firewall; Zabezpieczanie usług; Gromadzenie informacji dowodowej z wykonanych połączeń. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	03-12-2024	12:45	14:15	01:30	Tak
<p>13 z 22</p> <p>Przerwa.</p>	Jacek Herold	03-12-2024	14:15	14:30	00:15	Tak
<p>14 z 22</p> <p>Bezpieczeństwo współpracy z sieciami podmiotów partnerskich: Projektowanie i wdrażanie bezpiecznego dostępu do usług; Diagnostyka zabezpieczeń. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	04-12-2024	08:45	10:15	01:30	Tak
<p>15 z 22</p> <p>Przerwa.</p>	Jacek Herold	04-12-2024	10:15	10:30	00:15	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<p>16 z 22</p> <p>Ćwiczenia praktyczne z zakresu: Praktycznych scenariuszy konfiguracji sieciowych; Routingu w rozbudowanych sieciach. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	04-12-2024	10:30	12:00	01:30	Tak
<p>17 z 22</p> <p>Przerwa.</p>	Jacek Herold	04-12-2024	12:00	12:45	00:45	Tak
<p>18 z 22</p> <p>Ćwiczenia praktyczne z zakresu: Konfigurowanie bezpiecznego dostępu do usług w sieciach; Konfiguracji firewalli stateless i stateful. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	04-12-2024	12:45	14:15	01:30	Tak
<p>19 z 22</p> <p>Przerwa.</p>	Jacek Herold	04-12-2024	14:15	14:30	00:15	Tak
<p>20 z 22</p> <p>Bezpieczeństwo współpracy z sieciami podmiotów partnerskich: Zagadnienia bezpieczeństwa dostępu do usług; Sposoby udostępnienia usług. (Wykłady, dyskusja, ćwiczenia.)</p>	Jacek Herold	04-12-2024	14:30	16:00	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<div style="background-color: #e91e63; color: white; padding: 2px; display: inline-block; font-size: 0.8em;">21 z 22</div> Ćwiczenia praktyczne z zakresu: Bezpieczeństwo udostępnienia usług w sieciach publicznych; Ograniczania ruchu sieciowego. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	04-12-2024	14:30	15:30	01:00	Tak
<div style="background-color: #e91e63; color: white; padding: 2px; display: inline-block; font-size: 0.8em;">22 z 22</div> Walidacja.	-	04-12-2024	15:30	16:00	00:30	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 797,00 PLN
Koszt przypadający na 1 uczestnika netto	3 900,00 PLN
Koszt osobogodziny brutto	199,88 PLN
Koszt osobogodziny netto	162,50 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Jacek Herold

Sieci teleinformatyczne, audyty bezpieczeństwa, wsparcie techniczne.

Ponad 20 lat doświadczenia zawodowego. Bezpieczeństwa systemów operacyjnych i sieci. Audyty bezpieczeństwa w tym sektor bankowy - rekomendacja "D"KNF. 8 lat pracy w Wrocławskim Centrum Sieciowo Superkomputerowym WCSS.

Wykształcenie wyższe (mgr inż. elektroniki). Politechnika Wroclawska.
Ponad 3 500 godzin przeprowadzonych zajęć. Ponad 10 lat doświadczenia szkoleniowego.
Prowadzenie zajęć z zakresu bezpieczeństwa na Politechnice Wroclawskiej.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Całość opracowanych materiałów składa się z: opisów, wykresów, schematów, zdjęć i filmów. Po zakończeniu kształcenia wszyscy uczestnicy otrzymują materiały w formie skryptu dotyczące całości przekazywanej wiedzy.

Każdy uczestnik realizujący szkolenie w formie zdalnej w czasie rzeczywistym ma możliwość otrzymania od nas (za pośrednictwem kuriera) wyposażenia stanowiska szkoleniowego tj. jednostka sprzętowa wyposażona w dostęp do serwera z przygotowanym ekosystemem do wykonywania ćwiczeń oraz oprogramowanie tj. emulatory sieci i routerów oraz analizatory ruchu sieciowego Wireshark, Nmap i IPtables. Po zakończonym szkoleniu sprzęt zostaje odebrany przez kuriera.

Informacje dodatkowe

Faktura za usługę rozwojową podlega zwolnieniu z VAT dla osób korzystających z dofinansowania powyżej 70%.

Cena usługi jest ceną promocyjną obowiązującą od 19.04.2024 r. Cena nominalna- 4500 zł.

Szkolenie jest bardzo szczegółowe, ponieważ zależy nam na przekazaniu jak największej ilości informacji. Łącznie trwa 24 godzin dydaktycznych i prowadzone jest przez tydzień od poniedziałku do piątku, w godzinach od 8:45 do 16:00.

Harmonogram uwzględnia łączną liczbę godzin szkolenia, jako 21:45 godzin zegarowych, ponieważ uwzględnia również przerwy pomiędzy poszczególnymi blokami zajęć (I przerwa - 15 min, II przerwa - 45 min, III przerwa 15 min / 1 dzień).

Szkolenie rozpoczyna się pre-testem weryfikującym początkową wiedzę uczestnika usługi rozwojowej i zakończone jest wewnętrznym egzaminem (post-test) weryfikującym i potwierdzającym pozyskaną wiedzę, pozytywne jego zaliczenie honorowane jest certyfikatem potwierdzającym jego ukończenie i uzyskane efekty kształcenia.

Warunki techniczne

Warunki techniczne niezbędne do udziału w usłudze:

- Do połączenia zdalnego w czasie rzeczywistym pomiędzy uczestnikami, a trenerem służy program "Zoom Client for Meetings" (do pobrania ze strony <https://zoom.us/download>).
- Komputer/laptop z kamerką internetową z zainstalowanym klientem Zoom, minimum dwurdzeniowy CPU o taktowaniu 2 GHz.
- Mikrofon i słuchawki (ewentualnie głośniki).
- System operacyjny MacOS 10.7 lub nowszy, Windows 7, 8, 10, Linux: Mint, Fedora, Ubuntu, RedHat.
- Przeglądarkę internetowa: Chrome 30 lub nowszy, Firefox 27 lub nowszy, Edge 12 lub nowszy, Safari 7 lub nowsze.
- Dostęp do internetu. Zalecane parametry przepustowości łącza: min. 5 Mbps - upload oraz min. 10 Mbps - download, zarezerwowane w danym momencie na pracę zdalną w czasie rzeczywistym. Umożliwi to komfortową komunikację pomiędzy uczestnikami, a trenerem.
- Link umożliwiający dostęp do szkolenia jest aktywny przez cały czas jego trwania, do końca zakończenia danego etapu szkolenia. Każdy uczestnik będzie mógł użyć go w dowolnym momencie trwania szkolenia.

Adres

ul. Krzeczowska 20
32-700 Bochnia

woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt



Artur Kowalewski

E-mail szkolenia@notebookmaster.pl

Telefon (+48) 573 436 635