Możliwość dofinansowania

Szkolenie SO-B-08 Bezpieczeństwo sieci i testy penetracyjne

Numer usługi 2025/02/04/142469/2539613

2 214,00 PLN brutto
1 800,00 PLN netto
92,25 PLN brutto/h
75,00 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
20.05.2025 do 23.05.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie "Bezpieczeństwo sieci i testy penetracyjne" skierowane jest do specjalistów ds. bezpieczeństwa IT, administratorów systemów oraz audytorów, którzy chcą poszerzyć swoją wiedzę na temat testów penetracyjnych. Doskonale sprawdzi się również dla deweloperów, pragnących tworzyć bezpieczne aplikacje oraz osób początkujących w cyberbezpieczeństwie, posiadających podstawową znajomość sieci komputerowych. Program jest odpowiedni zarówno dla doświadczonych profesjonalistów, jak i tych, którzy dopiero zaczynają swoją karierę w tej dziedzinie. Dzięki praktycznym laboratoriom uczestnicy nabędą umiejętności identyfikacji i neutralizacji zagrożeń w rzeczywistych środowiskach IT. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	05-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24

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 Bezpieczeństwo sieci i testy penetracyjne jest przygotowanie uczestnika do samodzielnego tworzenia środowisk testowych do testów penetracyjnych oraz opanowanie metodologii przeprowadzania testów bezpieczeństwa i zabezpieczania infrastruktury IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się wiedzą dotyczącą bezpieczeństwa informacji oraz identyfikacji popularnych zagrożeń.	Charakteryzuje podstawowe elementy bezpieczeństwa informacji. Rozróżnia dokumenty dobrej praktyki (NIST, NSC). Definiuje najczęściej spotykane zagrożenia cybernetyczne.	Test teoretyczny
Uczestnik tworzy środowisko testowe do przeprowadzania testów penetracyjnych.	Konfiguruje sieć wirtualną z usługą Active Directory. Instaluje systemy testowe, takie jak Metasploitable, DVWA, Windows Server. Buduje laboratorium do testowania aplikacji webowych.	Test teoretyczny
Uczestnik analizuje i testuje podatności sieci WLAN, w tym protokołu WPA2.	Rozpoznaje słabości protokołów WPA/WPA2. Wykorzystuje narzędzia do testowania sieci bezprzewodowych (np. Kismet, Aircrack-ng). Przeprowadza testy łamania klucza PSK w sieciach WPA2-PSK.	Test teoretyczny
Uczestnik identyfikuje i przeprowadza ataki na aplikacje webowe, w tym podatności XSS.	Rozróżnia typy podatności XSS (reflected, stored, DOM). Wykorzystuje narzędzia BeEF oraz Metasploit do przeprowadzania ataków XSS. Analizuje wyniki testów i proponuje odpowiednie środki zaradcze.	Test teoretyczny
Uczestnik przeprowadza testy podatności SQL injection na aplikacje webowe.	Rozpoznaje różne techniki SQL injection. Używa narzędzi takich jak SQLmap, SQLNinja do wykrywania podatności. Przeprowadza testy w środowisku DVWA i analizuje wyniki.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik przełamuje zabezpieczenia zdalnego dostępu (RDP, SSH, FTP).	Rozpoznaje luki w zabezpieczeniach protokołów zdalnego dostępu. Używa narzędzi takich jak Hydra, Medusa, Metasploit do testów ataków brute force. Analizuje skuteczność przeprowadzonych ataków.	Test teoretyczny
Uczestnik identyfikuje i przeprowadza ataki na systemy operacyjne Windows i Active Directory.	Zbiera poświadczenia i przeprowadza ataki SMB relay. Wykorzystuje narzędzia impacket-secretsdump, hashcat, John the Ripper do łamania haseł. Przeprowadza ataki typu Pass-the-Hash oraz podnoszenie uprawnień w Active Directory.	Test teoretyczny
Uczestnik analizuje i testuje bezpieczeństwo połączeń SSL.	Rozpoznaje luki w zabezpieczeniach SSL/TLS. Wykorzystuje narzędzia takie jak Testssl, nmap NSE do analizy połączeń SSL. Przeprowadza ataki typu man-in-the-middle i analizuje ich skutki.	Test teoretyczny
Uczestnik zwiększa poziom bezpieczeństwa systemów Windows i Linux.	Konfiguruje centralną archiwizację logów (Eventlog, rsyslog). Używa narzędzi z pakietu Sysinternals Suite (AccessChk, Procmon). Konfiguruje zabezpieczenia SELinux oraz Fail2ban.	Test teoretyczny
Uczestnik przeprowadza analizę i audyt zabezpieczeń sieci oraz systemów.	Tworzy raport z wynikami testów penetracyjnych. Proponuje odpowiednie środki zaradcze na wykryte podatności. Przedstawia rekomendacje dotyczące poprawy zabezpieczeń infrastruktury IT.	Test teoretyczny
Współpracuje z innymi członkami zespołu w organizacji, korzystając z narzędzi do pracy grupowej w celu realizacji wyznaczonego celu lub projektu	Identyfikuje wyzwania związane z wyznaczonym celem, planuje etapy ich realizacji, monitoruje ich wykonanie oraz ocenia ich efektywność. Współdzieli informacje z innym współpracownikami i wykorzystuje narzędzia do pracy nad danymi w ramach zespołów.	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, Uczestnik szkolenia, poza certyfikatem, otrzymuje zaświadczenie o ukończeniu szkolenia z zawartym opisem efektów 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

Nasze szkolenie "Bezpieczeństwo sieci i testy penetracyjne" nie tylko dostarcza teoretycznej wiedzy, ale także praktycznych umiejętności w dziedzinie cyberbezpieczeństwa. Zyskasz unikalną szansę nie tylko na zrozumienie podstawowych aspektów bezpieczeństwa, ale także na praktyczne doświadczenie w testowaniu penetracyjnym. Oferujemy praktyczne narzędzia i scenariusze laboratoryjne, abyś mógł skutecznie stosować zdobytą wiedzę w realnych sytuacjach. Celem szkolenia Bezpieczeństwo sieci i testy penetracyjne jest przygotowanie uczestnika do samodzielnego tworzenia środowisk testowych do testów penetracyjnych oraz opanowanie metodologii przeprowadzania testów bezpieczeństwa i zabezpieczania infrastruktury IT.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informacje na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Przed rozpoczęciem szkolenia Uczestnik rozwiązuje pre-test badający poziom wiedzy na wstępie.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy.

Szkolenie trwa **24 godziny dydaktyczne** (1 godz. dydaktyczna = 45 minut), tj. 18 godzin zegarowych i jest realizowane w ciągu 3 dni.

Czas trwania przerw nie wlicza się do ogólnej liczby godzin trwania usługi.

Trener ma możliwość przesunięcia przerw, tak aby dostosować harmonogram do potrzeb uczestników.

Szkolenie jest prowadzone na żywo (on-line), na platformie Microsoft Teams.

Wstęp do bezpieczeństwa informacji

Elementy wchodzące tradycyjnie w zakres bezpieczeństwa informacji.

Dokumenty opisujące dobre praktyki (NIST/NSC)

Popularne rodzaje zagrożeń

Tworzenie środowisk testowych do testów penetracyjnych

Koncepcyjny przegląd testów bezpieczeństwa

Metodologia przeprowadzania testów

Zapoznanie z dystrybucją Kali Linux

Budowanie środowiska testowego

Konfigurowanie sieci wirtualnej z usługą Active Directory

Instalowanie zdefiniowanych celów

Tworzenie laboratorium do testowania aplikacji webowych

Laboratorium*: Przygotowanie środowiska Metasploitable i DVWA oraz Windows 10/Windows Server.*

Ataki na infrastrukturę sieci WLAN – podatności WPA2

Szyfrowanie w sieciach WLAN

Standard WPA/WPA2

Narzędzia do testowania sieci bezprzewodowych Kismet, airmon-ng, airodump-ng, aireplay-ng, wifite2, hashcat, aircrack-ng, genpmk itp.

Laboratorium: *Łamanie klucza PSK w sieciach z szyfrowaniem WPA2- PSK*

Bezpieczeństwo aplikacji webowych - podatność XSS

Typy podatności XSS

Non-persistent (reflected) XSS

Persistent (stored) XSS

DOM XSS

Omówienie narzędzi BeEF oraz Metasploit oraz innych narzędzi do testowania podatności aplikacji internetowych (Burp Suite, ZAP)

Uruchamianie i obsługa interfejsu programu BeEF

Moduły programu BeEF

Konsola programu Metasploit – uruchamianie testów, przygotowanie ładunków

Przeprowadzanie ataków typu XSS za pomocą pakietu BeEF

Laboratorium: *Przeprowadzanie ataków typu XSS za pomocą pakietu BeEF w środowisku testowym, na przeglądarki i infrastrukturę sieciową.*

Bezpieczeństwo aplikacji webowych - podatność SQL

Omówienie podatności SQL injection

Wybrane narzędzia do testowania SQL injection

Laboratorium: *Przeprowadzanie ataków typu SQL injection za pomocą pakietu SQLmap, SQLNinja, jSQL Injection w środowisku testowym DVWA.*

Ataki na zdalny dostęp

Luki w zabezpieczeniach protokołów komunikacyjnych

Przełamywanie zabezpieczeń protokołu RDP

Przełamywanie zabezpieczeń protokołu SSH,FTP

Przełamywanie zabezpieczeń protokołu POP3,SMTP

Laboratorium *: Zastosowanie narzędzi hydra, medusa, metasploit do ataków na zdalny dostęp*

Ataki na zabezpieczenia systemu operacyjnego Windowsi AD

Zbieranie poświadczeń i podnoszenie uprawnień

Ataki typu SMB relay

Łamanie zabezpieczeń SAM i Active Directory z impacket-secretsdump, ataki typu offline

Ataki z wykorzystaniem pozyskanych hash'y (Pass-the-Hash) - impacket-psexec

Podnoszenie uprawnień w Active Directory

Omówienie narzędzia mimikatz

Laboratorium *: Zastosowanie narzędzi impacket-secretsdump, impacket-psexec, hashcat, John the Ripper, metasploit do ataków na zabezpieczenia systemu Windows i AD*

Ataki na połączenia SSL

Słabe strony i luki w zabezpieczeniach protokołu SSL

Praca z programem Testssl

Rozpoznawanie połączeń SSL

Atak man-in-the-middle

Laboratorium *: Użycie programem testssl oraz skryptów nmap NSE, ssl-cert, ssl-enum-ciphers, sslv2, sslcaudit, sslscan, tlssled.***Wybrane zagadnienia z zwiększania bezpieczeństwa systemu Windows i Linux**

Eventlog, Event Forwarding – ustawienia, centralna archiwizacja logów

Rsyslog - ustawienia, centralna archiwizacja logów

Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon

SELinux - Security-Enhanced Linux

Fail2ban – ochrona przed atakami online, słownikowe i brute force

Windows Defender - ograniczenie podatności na atak

Laboratorium : *Konfiguracja logowania zdarzeń i serwera logów, SELinux,*

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania się minimalnej liczby Uczestników tj. 3 osób.

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 Wstęp do bezpieczeństwa informacji (on-line, na żywo, wykład)	Zdzisław Knap	20-05-2025	09:00	10:30	01:30
2 z 22 Przerwa	Zdzisław Knap	20-05-2025	10:30	10:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 22 Tworzenie środowisk testowych do testów penetracyjnych (on-line, na żywo, wykład)	Zdzisław Knap	20-05-2025	10:45	12:15	01:30
4 z 22 Przerwa	Zdzisław Knap	20-05-2025	12:15	12:30	00:15
5 z 22 Tworzenie środowisk testowych do testów penetracyjnych (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	20-05-2025	12:30	14:00	01:30
6 z 22 Przerwa	Zdzisław Knap	20-05-2025	14:00	14:30	00:30
7 z 22 Ataki na infrastrukturę sieci WLAN – podatności WPA2 (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	20-05-2025	14:30	16:00	01:30
8 z 22 Bezpieczeństwo aplikacji webowych - podatność XSS (on-line, na żywo, wykład)	Zdzisław Knap	21-05-2025	09:00	10:30	01:30
9 z 22 Przerwa	Zdzisław Knap	21-05-2025	10:30	10:45	00:15
10 z 22 Bezpieczeństwo aplikacji webowych - podatność XSS (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	21-05-2025	10:45	12:15	01:30
11 z 22 Przerwa	Zdzisław Knap	21-05-2025	12:15	12:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 22 Bezpieczeństwo aplikacji webowych - podatność SQL (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	21-05-2025	12:30	14:00	01:30
13 z 22 Przerwa	Zdzisław Knap	21-05-2025	14:00	14:30	00:30
14 z 22 Ataki na zdalny dostęp (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	21-05-2025	14:30	16:00	01:30
15 z 22 Ataki na zabezpieczenia systemu operacyjnego Windows i AD (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	23-05-2025	09:00	10:30	01:30
16 z 22 Przerwa	Zdzisław Knap	23-05-2025	10:30	10:45	00:15
17 z 22 Ataki na połączenia SSL (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	23-05-2025	10:45	12:15	01:30
18 z 22 Przerwa	Zdzisław Knap	23-05-2025	12:15	12:30	00:15
19 z 22 Wybrane zagadnienia z zwiększania bezpieczeństwa systemu Windows i Linux (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	23-05-2025	12:30	14:00	01:30
20 z 22 Przerwa	Zdzisław Knap	23-05-2025	14:00	14:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 22 Wybrane zagadnienia z zwiększania bezpieczeństwa systemu Windows i Linux (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	23-05-2025	14:30	15:45	01:15
22 z 22 Walidacja (post-test)	-	23-05-2025	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 214,00 PLN
Koszt przypadający na 1 uczestnika netto	1 800,00 PLN
Koszt osobogodziny brutto	92,25 PLN
Koszt osobogodziny netto	75,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Zdzisław Knap

Doświadczony Trener i wykładowca, z 20-letnim doświadczeniem. Certyfikowany Akademicki Instruktor Novell NAI w zakresie Novell Netware i Suse Linux.
Poza branżowymi certyfikatami produktowymi posiada akredytacje trenerskie m.in Microsoft Certified Trainer MCT , Novell Academic Instruktor, Certyfikowany Trener CompTIA, Linux Professional Institute (LPI). Specjalizuje się w technologiach Linux, Microsoft oraz w zakresie cyberbezpieczeństwa. Jego umiejętności interpersonalne oraz szeroka wiedza merytoryczna jest wysoko oceniana przez uczestników.
Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane materiały szkoleniowe w formie elektronicznej (ebook) oraz dostęp do środowiska laboratoryjnego online.

Warunki uczestnictwa

Przed przystąpieniem do szkolenia uczestnik powinien posiadać podstawową znajomość systemów operacyjnych Windows, wiedzę z zakresu podstawowych koncepcji związanych z sieciami komputerowymi oraz znać podstawy bezpieczeństwa IT.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

kompetencja związana z cyfrową transformacją;

UWAGA! Przed dokonaniem zgłoszenia / złożeniem wniosku o dofinansowanie prosimy o kontakt z SOFTRONIC w celu potwierdzenia terminu szkolenia oraz dostępności miejsc: e-mail: softronic@softronic.pl lub tel. 61 865 88 40

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział zkażdego miejsca na świecie.

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.

- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.

- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+

- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840