Możliwość dofinansowania

Szkolenie SO-B-08 Bezpieczeństwo sieci i testy penetracyjne

Numer usługi 2024/11/18/142469/2417474

2 952,00 PLN brutto
2 400,00 PLN netto
123,00 PLN brutto/h
100,00 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
11.12.2024 do 13.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	04-12-2024
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 jest dostarczenie uczestnikom zaawansowanej wiedzy oraz praktycznych umiejętności z zakresu testów penetracyjnych i zabezpieczania infrastruktury IT. Uczestnicy nauczą się wykrywać i identyfikować podatności w systemach oraz aplikacjach, a także efektywnie reagować na zagrożenia cybernetyczne.

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
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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
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

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" wyróżnia się jako kompleksowy program, który 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.

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 informację 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 zegarowe i jest realizowane w ciągu 3 dni.

W trakcie każdego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

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 Windows i 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: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 952,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	123,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały.

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;

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego 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, ktory potwierdzi swój udziałw 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/glosniki 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