C)PTE - Certified Penetration Testing Engineer

Usługa archiwalna

Informacje o usłudze

Czy usługa może być dofinansowana?	Tak
Sposób dofinansowania	• wsparcie dla osób indywidualnych • wsparcie dla przedsiębiorców i ich pracowników
Rodzaj usługi	Usługa szkoleniowa
Podrodzaj usługi	Usługa szkoleniowa
Dostępność usługi	Otwarta

Numer usługi		**2019/04/26/10100/383815**	
Cena netto	**5 215,00 zł**	Cena brutto	**5 215,00 zł**
Cena netto za godzinę	**149,00 zł**	Cena brutto za godzinę	**149,00**
Usługa z możliwością dofinansowania		**Tak**	
Liczba godzin usługi		**35**	
Termin rozpoczęcia usługi	**2019-12-09**	Termin zakończenia usługi	**2019-12-13**
Termin rozpoczęcia rekrutacji	**2019-04-26**	Termin zakończenia rekrutacji	**2019-12-09**
Maksymalna liczba uczestników		12	
Kategoria główna KU		**Informatyka i telekomunikacja**	
Kategorie dodatkowe KU		**Informatyka i telekomunikacja**	

Podstawa uzyskania wpisu w zakresie świadczenia usług współfinansowanych	**Certyfikaty:** Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES)
Czy usługa pozwala na uzyskanie kwalifikacji lub części kwalifikacji zarejestrowanych w ZRK?	**Nie**
Czy usługa pozwala na uzyskanie kwalifikacji innych niż kwalifikacje zarejestrowane w ZRK?	**Nie**
Czy usługa prowadzi do nabycia kompetencji?	**Tak**

Informacje o podmiocie świadczącym usługę

Nazwa podmiotu		**Compendium - Centrum Edukacyjne Spółka z o.o.**	
Osoba do kontaktu	**Michał Dobrzański**	Telefon	**12 29 84 777**
E-mail	**michal.dobrzanski@compendium.pl**		

Cel usługi

Cel edukacyjny

Szkolenie Certified Penetration Testing Engineer dostarcza praktyczną wiedzę na temat bezpieczeństwa IT, która w szczególności pozwala na wyszukiwanie podatności systemów, rozpoznawania luk w systemach bezpieczeństwa, identyfikowanie słabości i ochronę przed potencjalnymi zagrożeniami. Uczestnicy szkolenia poznają sztukę etycznego hackowania w profesjonalnych ramach prowadzenia testów penetracyjnych. Podstawą kursu CPTE są zajęcia praktyczne bazujące na metodyce testów penetracyjnych stosowanej przez międzynarodową grupę ekspertów ds. podatności systemów współpracującej z Mile2. Również autoryzowani trenerzy Mile2 to praktycy, dzięki temu łączą wiedze teoretyczną z nabywanym doświadczeniem rzeczywistym a to w konsekwencji zapewnia skuteczny transfer wiedzy do uczestników szkolenia. Zawartość kursu CPTE bazuje na 5 kluczowych elementach testów penetracyjnych: zbieranie informacji, skanowanie, enumeracja, eksploracja i raportowanie. Wykrywanie najbardziej aktualnych podatności jest zawsze przeprowadzenia za pomocą wypróbowanych i realnie stosowanych technik. Kurs ten rozwija również umiejętności biznesowe, które są niezbędne do określenia możliwości stosowanej ochrony, uzasadniania potrzeby przeprowadzania testów i optymalizacji systemów bezpieczeństwa z punktu widzenia procesów biznesowych danej organizacji i redukcji zagrożeń z nich wynikających. Mile2 w zakresie szkolenia CPTE zdecydowanie wykracza poza naukę tego jak „hackować” – uczestnicy szkolenia powinni być przede wszystkim przygotowani na naukę przeprowadzania testów penetracyjnych z wykorzystaniem zawansowanych ustandaryzowanych technik wykrywania zagrożeń przy równoczesnym stosowaniu najbardziej etycznych metod hackerskich. Osoby bardziej zainteresowane samymi technikami etycznego włamywania niż metodyką prowadzenia testów penetracyjnych odsyłamy do szkolenia CPEH. Po ukończeniu szkolenia: Uczestnicy kursu CPTE będą mogli bez najmniejszych obaw przystąpić do certyfikacyjnego egzaminu CPTE co jest szczególnie rekomendowane. Dodatkowo będą posiadać głęboką wiedzę i umiejętności z zakresu metodyki prowadzenia testów penetracyjnych i sprawdzonych technik etycznego hackowania zdobytą w oparciu o bieżąco aktualizowane materiały i laboratorium szkoleniowe (materiały i laboratorium dostosowywane do nowo pojawiających się zagrożeń i dostępnych narzędzi), które zostały opracowane przez międzynarodową grupę ekspertów UWAGA: NSA (The National Security Agency) akredytowała kurs C)PTE jako spełniający standard: CNSSI-4013 National Information Assurance Training Standard for System Administrators

Szczegółowe informacje o usłudze

Ramowy program usługi

- Logistyka testów penetracyjnych:
  - Czym jest test penetracyjny?
  - Zalety płynące z przeprowadzania pentestu
  - Ubezpieczenia od włamań
  - Ankieta CSI Computer Crime
  - Przegląd najnowszych ataków i włamań komputerowych
  - Ile firmę kosztuje udany atak hackera?
  - IC3 (Internet Crime Complaint Center)
  - Ciągła ewolucja zagrożeń
  - Cykl życia podatności w zabezpieczeniach
  - Czas życia exploitów
  - Definicja zombie
  - Czym jest botnet?
  - Budowa botnetu

    - Statystyki botnetów
    - Rozbudowa botnetów
    - Typy testów penetracyjnych
    - Metodologie pentestów
    - Różnica między hackerem a pentesterem
    - Narzędzia wykorzystywane przez włamywaczy
    - Narzędzie: SecurityNOW! SX
    - Błędy popełniane przez zarząd
- Podstawy Linuxa
    - Historia Linuxa
    - System operacyjny GNU
    - Wstęp do Linuxa
    - Środowiska graficzne
    - Linia poleceń
    - Książki o Linuxie
    - Formaty plików z danymi o użytkownikach i ich hasłami
    - Zarządzanie kontami użytkowników
    - Zmiana hasła użytkownika
    - Konfiguracja interfejsów sieciowych
    - Montowanie dysków
    - Archiwa i kompresja danych
    - Kompilacja programów
    - Wykorzystanie Boot CD
    - Przegląd popularnych dystrybucji
    - Kali Linux
- Zbieranie informacji
    - Informacje gromadzone przez atakujących
    - Organizacja zebranych informacji
    - Edytor Leo
    - Free Mind: mapa myśli
    - IHMC CmapTools
    - Metody pozyskiwania informacji
    - Dostęp fizyczny
    - Socjotechnika
    - Sieci społecznościowe
    - Komunikatory internetowe oraz czat
    - Dostęp cyfrowy
    - Rekonesans pasywny oraz aktywny
    - Footprinting
    - Maltego
    - FireCAT
    - Google hacking
    - Google i operatory
    - SiteDigger
    - Ogłoszenia o pracę
    - Blogi i fora
    - Grupy google
    - Archiwum Intrnetu: WayBack Machine
    - DNS
    - WHOIS
    - nslookup oraz dig
    - traceroute i traceroute 3D

    - wyszukiwarki osób
    - Intelius
    - EDGAR
    - Netcraft
    - Zapobieganie udostępnianiu nadmiaru informacji
    - domainsbyproxy.com
- Wykrywanie systemów
    - Wstęp do skanowania portów
    - Sztuczki podczas skanowania portów
    - Przegląd skanerów
    - Online ping
    - Technika wykrywania czy host jest online
    - Skany typu half-open
    - Porty blokowane przez firewall
    - Wykrywanie wersji usługi
    - Skanowanie za pomocą protokołu UDP
    - Zaawansowane techniki
    - Omówienie narzędzi: Superscan, Look@LAN, Hping2, Auto Scan, Xprobe2, p0f, amap
    - Fragmentacja pakietów
    - Ochrona przed skanowaniem portów
- Enumeracja
    - Banery
    - Narzędzia do pozyskiwania informacji z banerów
    - Enumeracja DNS
    - Transfer strefy
    - Niebezpieczeństwa związane z SNMP
    - Enumeracja ActiveDirectory
    - Null sessions
    - Narzędzie: Cain and Abel
    - Narzędzie: THC-Hydra
- Wykrywanie podatności
    - Podatności w sieciach i usługach
    - Wstęp do wykrywania i raportowania podatności
    - Automatyzacja podczas wykrywania i raportowania podatności
    - SAINT
    - Nessus
    - Retina
    - Qualys Guard
    - LANguard
    - Microsoft Baseline Analyzer
    - Analiza wyników działania skanerów
    - Zarządzanie systemem łatek
- Malware
    - Dystrybucja malware
    - Możliwości malware
    - Monitorowanie metod automatycznego startu programów i usług
    - Narzędzie: netcat
    - Narzędzie: Restorator
    - Narzędzie: Exe Icon
    - Trojan: Backdoor.Zombam.B
    - Trojan: JPEG GDI+
    - Zdalne Exploity

    - Unikanie wykrycia przez trojany
    - BPMTK
    - Zapobieganie działaniu malware
    - Gargoyle Investigator
    - Spy Sweeper Enterprise
    - CM Tool
    - Edukacja użytkowników końcowych
- Ataki na systemy operacyjne Windows
    - Ataki na hasła użytkowników
    - Zasada szyfrowania haseł algorytmem LM
    - Zasada szyfrowania haseł algorytmem NT
    - Tablice tęczowe
    - NTPASSWD – wstrzykiwanie haseł
    - Podsłuchiwanie haseł
    - Protokoły uwierzytelniania w Windows
    - Kerbsniff i Kerbcrack
    - Monitorowanie logów
    - Zabezpieczenie dysku twardego
    - Łamanie zabezpieczeń dysku twardego
    - Tokeny i smard cards
    - Tokeny USB
    - Zakrywanie śladów
    - Wyłączenie audytu
    - Czyszczenie logów
    - NTFS Alternate Data Streams
    - Stenografia
    - TOR – opis działania
    - TOR + OpenVPN = Janus VM
    - Narzędzie: RootKit
    - Ochrona przed RootKit
- Ataki na systemy operacyjne Linux
    - System plików
    - Jądro
    - Procesy
    - Konta użytkowników i grupy
    - Struktura plików z informacjami o użytkownikach i hasłami
    - Uprawnienia
    - Logi i audyt
    - Popularne usługi sieciowe
    - Ataki zdalne
    - Ataki typu brute-force
    - Ochrona przed atakami brute-force
    - Ataki i ochrona udziałów NFS
    - Ataki na hasła użytkowników, ochrona, solenie
    - Dowiązania twarde oraz miękkie
    - Biblioteki współdzielone
    - Luki bezpieczeństwa w jądrze systemu
    - Czyszczenie logów
    - Rootkity i ochrona przed nimi
- Techniki wykorzystywane przez exploity
    - Zasada działania exploitów
    - Format Strings

    - Race Conditions
    - Organizacja pamięci
    - Ataki typu Buffer OverFlows
    - Ataki typu Heap OverFlows
    - Etapy rozwoju explitów
    - Shellcode
    - Metasploit Framework
    - Meterpreter
    - Fuzzery
    - SaintExploit
    - Core Impact
- Ataki na sieci bezprzewodowe
    - standardy sieci bezprzewodowych
    - SSID
    - Filtrowanie adresów MAC
    - WEP i jego podatności
    - Podstawy szyfrowania XOR
    - WPA
    - TKIP
    - Podatności protokołu WPA
    - 802.11i – WPA2
    - WPA2-PSK
    - LEAP i jego podatnościach
    - NetStumbler
    - Narzędzia: Kismet, Aircrack-ng
    - Ataki typu deauth / diassociate
    - Ataki na sieci zabezpieczone WEP i WPA
    - narzędzie: coWPAtty
    - Ataki na CISCO LEAP
    - Narzędzia: asleap, WiFiZoo, Ersside-ng
    - 802.1X
    - Wady i zalety EAP
    - Rozwiązania firmy Aruba
    - RAPIDS Rouge AP Detection
- Sieci, podsłuchiwanie, IDS
    - podsłuchiwanie pakietów
    - Narzędzia: Pcap, WinPcap, Wireshark
    - Odbudowa strumienia TCP
    - Narzędzia: Pacektyzer, tcpdump, windump, OmniPeek
    - Wykrywanie podsłuchu pakietów
    - Metody aktywnego podsłuchiwania pakietów
    - Ataki na switche
    - Ataki na tablice ARP
    - Narzędzia: Cain and Abel, Ettercap, Dsniff
    - DNS Spoofing
    - Kradzież sesji
    - Rozszywanie sesji SSL
    - Ataki na VoIP
    - Przechwytywanie sesji RDP
    - Omijanie firewalli i unikanie wykrycia przez IDS
    - Rozwój firewalli
    - SPS (Spyware Prevention System)

- Ataki na bazy danych
    - Podatności i najpopularniejsze ataki
    - Wstrzyknięcia kodu SQL
    - Enumeracja baz danych
    - SQL Extended Stored Procedures
    - Ataki bezpośrednie
    - Właściwości połączeń SQL
    - Ataki na serwery z bazami danych
    - Narzędzia: SQLScan, sql, Query Analyzers, SQLExec
    - Metasploit
    - Odkrywanie dziur i ich łatanie
    - Utwardzanie baz danych
- Ataki na aplikacje webowe
    - Popularne zagrożenia aplikacji webowych
    - Anatomia ataków na aplikacje webowe
    - Elementy składowe webaplikacji
    - Metodologie testów penetracyjnych
    - URL mapping
    - Formy komunikacji z aplikacją
    - Modyfikacja przesyłanych parametrów
    - Ataki XSS
    - Wstrzyknięcia kodu
    - Brak walidacji danych wejściowych
    - Ataki na serwer IIS
    - Podróżowanie po katalogach
    - Unicode
    - N-Stalker Scanner
    - NTOSpider
    - Wikto
    - SiteDigger
    - Lokalne proxy: Paros, Burp
    - Ataki siłowe: Brutus
    - Ciasteczka
    - Acunetix Web Scanner
    - Samurai Web Testing Framework
- Dokumentacja projektu
    - Tworzenie raportu
    - Kryteria raportu
    - Analiza ryzyka
    - Tabela z wynikami
    - Tabela z odkrytymi podatnościami
    - Forma dostarczenia raportu
    - Zalecenia
    - Podsumowanie dla zarządu
    - Raport techniczny
    - Spis treści
    - Zakres przeprowadzonych testów
- Dodatki
    - Zrozumienie testów penetracyjnych
    - Regulacje sektora finansowego
    - Kontrola dostępu
    - Protokoły

- Kryptografia
- Ekonomia i prawo

Efekty usługi (produkty), efekty uczenia się/kształcenia

Samodzielne wyszukiwanie podatności systemów, rozpoznawania luk w systemach bezpieczeństwa, identyfikowanie słabości i ochronę przed potencjalnymi zagrożeniami

Grupa docelowa

Usługa również adresowana dla uczestników projektu **Kierunek Kariera**

Materiały dydaktyczne

Autoryzowane materiały szkoleniowe Mile2

Harmonogram

LP	Przedmiot / Temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1	Biznesowa i techniczna logistyka testów penetracyjnych Podstawy systemu Linux Zbieranie informacji Wykrywanie systemów	2019-12-09	10:00	17:00	7:00
2	Enumeracja Wykrywanie podatności Malware Ataki na systemy Windows Ataki na systemy UNIX/Linux Zaawansowane techniki wykorzystywania Testowanie sieci bezprzewodowych Podsłuchiwanie sieci i systemy IDS Ataki na bazy danych Ataki na aplikacje webowe	2019-12-10	09:00	16:00	7:00
3	Dokumentacja i tworzenie raportu Zabezpieczanie systemów Windows - Powershell Przeprowadzenie testów przy pomocy Powershell	2019-12-11	09:00	16:00	7:00
4	Wprowadzenie do środowiska laboratoryjnego Podstawy systemu Linux Korzystanie z narzędzi do raportowania Zbieranie informacji Wykrywanie systemów Enumeracja Wykrywanie podatności	2019-12-12	09:00	16:00	7:00

LP	Przedmiot / Temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5	Malware Atakowanie systemów Windows Atakowanie systemów Linux / Unix Zaawansowane techniki wykrywania podatności i ich wykorzystywania Podsłuchiwanie sieci i systemy IDS Atakowanie baz danych Atakowanie aplikacji webowych	2019-12-13	09:00	16:00	7:00

Osoby prowadzące usługę

Imię i nazwisko	**Adam Jakubiec**
Obszar specjalizacji	Bezpieczeństwo IT
Doświadczenie zawodowe	Autoryzowany Trener MILE2, z wieloletnim doświadczeniem.
Doświadczenie w świadczeniu tego typu usług	Autoryzowany Trener MILE2, z wieloletnim doświadczeniem.
Wykształcenie	Wyższe

Lokalizacja usługi

Adres: **Tatarska 5** **30-103 Kraków, woj. małopolskie** Szczegóły miejsca realizacji usługi:	Warunki logistyczne: **Klimatyzacja,Laboratorium komputerowe,Wi-fi**