Karta usługi została zablokowana. Podmiot nie dopełnił wymagań związanych z publikacją karty usługi w Bazie Usług Rozwojowych. Zapis na usługę nie jest możliwy.

Techniki hackingu i cyberprzestępczości - Poziom 2 Ataki na systemy i sieci

Usługa archiwalna

Usluga została zablokowana przez Administratora Bazy.

Informacje o usłudze

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

Numer usługi		**2019/11/05/17164/482911**	
Cena netto	**3 890,00 zł**	Cena brutto	**4 784,70 zł**
Cena netto za godzinę	**185,24 zł**	Cena brutto za godzinę	**227,84**
Usługa z możliwością dofinansowania		**Tak**	
Liczba godzin usługi		**21**	
Termin rozpoczęcia usługi	**2020-03-03**	Termin zakończenia usługi	**2020-03-05**

Termin rozpoczęcia rekrutacji	**2020-01-31**	Termin zakończenia rekrutacji	**2020-02-26**
Maksymalna liczba uczestników		8	
Kategoria główna KU		**Informatyka i telekomunikacja**	
Kategorie dodatkowe KU		**Informatyka i telekomunikacja**	
Podstawa uzyskania wpisu w zakresie świadczenia usług współfinansowanych		**Certyfikaty:** Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych	
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		**Dagma sp. z o.o.**	
Osoba do kontaktu	**Ewelina Saracka**	Telefon	**+48327931120**
E-mail	**szkolenia@dagma.pl**		

Cel usługi

Cel edukacyjny

Głównym celem szkolenia jest zdobycie wiedzy na temat technik jakimi posługują się przestępcy w cyfrowym świecie, aby lepiej zabezpieczyć firmową infrastrukturę IT. Uczestnik szkolenia nabędzie umiejętności odnośnie obrony przed atakami na systemy operacyjne, zdobędzie wiedzę na temat postincydentalnych sposobów analizy skompromitowanych jednostek w sieci. Po ukończeniu szkolenia uczestnik ma praktyczną wiedzę z zakresu bezpieczeństwa systemów operacyjnych oraz sieci informatycznych, zna nowoczesne techniki internetowych włamywaczy, potrafi dobrać właściwe metody ochrony przed konkretnymi cyberatakami, potrafi analizować przebieg cyberataków i neutralizować je w zarodku. Po ukończeniu szkolenia uczestnik ma umiejętność samokształcenia się oraz potrafi umiejętnie rozstrzygać dylematy związane z codzienną pracą.

Szczegółowe informacje o usłudze

Ramowy program usługi

PROGRAM SZKOLENIA

1. WHOIS i wyliczanie DNS
2. Wykorzystywanie zaawansowanego oprogramowania do automatyzacji pracy
3. Wehikuł czasu stron internetowych
4. Budowa własnych pakietów od podstaw
5. Zaawansowane skanowanie jednostek w warstwie 2, 3 i 4 z wykorzystaniem szerokiej gamy dostępnych narzędzi
6. Identyfikowanie usług sieciowych oraz banerów aplikacji
7. Identyfikacja systemów oraz zapór sieciowych
8. Skanowanie TCP / UDP / zombie
9. Ataki na systemy operacyjne Windows, Linux, MacOS
10. Atakowanie poprzez błędy w oprogramowaniu JAVA, Winamp, Flash DLL
11. Szybka identyfikacja możliwych ataków - Windows Exploit Suggester
12. Ataki na powłokę bash – BashShelshock
13. Hakowanie kiosków internetowych
14. Ataki DoS/DDoS z wykorzystaniem serwerów DNS (DNS amplification)
15. Ataki DoS/DDoS typu buffer overflow
16. Ataki DoS/DDoS syn Flood
17. Ataki DoS/DDoS Sockstress
18. Omijanie blokad w sieci metodą tunelowania połączeń
19. Ataki Honeypot i Misassociation
20. Ataki Hirte
21. Ataki na protokół PEAP
22. Ataki na protokół EAP-TTLS
23. Ataki socjotechniczne

Efekty usługi (produkty), efekty uczenia się/kształcenia

- zdobycie umiejętności skutecznego zabezpieczenia urządzeń w sieci teleinformatycznej;
- zdobycie umiejętności analizowania przebiegu cyberataków;
- poznanie nowoczesnych technik internetowych włamywaczy;
- skuteczne zabezpieczenie firmowej infrastruktury IT przed atakami na systemy operacyjne;
- zrozumienie sposobu działania cyberprzestępców;
- zdobycie wiedzy na temat skutecznej obrony przed atakami;
- poznanie najlepszych metod przeciwdziałania i zapobiegania atakom.

Grupa docelowa

Szkolenie przeznaczone dla osób, które zajmują się bezpieczeństwem IT w firmie, jak również dla wszystkich osób chcących poszerzyć swoją wiedzę z zakresu bezpieczeństwa informatycznego.

Wymagana:

- Znajomośc podstaw Linuxa, działania sieci, zasady działania systemów
- Wiedza ze szkolenia **Techniki hackingu i cyberprzestępczości - Poziom 1 Wprowadzenie do hackingu w praktyce**

Opis warunków uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **www.acsdagma.com.pl** w celu

rezerwacji miejsca.

Materiały dydaktyczne

- pakiet materiałów szkoleniowych;
- zaświadczenie ACS Dagma dla każdego uczestnika;
- 14-dniowy kontakt z trenerem po szkoleniu.

Harmonogram

LP	Przedmiot / Temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1	Dzień I	2020-03-03	09:00	16:00	7:00
2	Dzień II	2020-03-04	09:00	16:00	7:00
3	Dzień III	2020-03-05	09:00	16:00	7:00

Osoby prowadzące usługę

Lokalizacja usługi

Adres: **ul. Bażantów 6a/3** **40-668 Katowice, woj. śląskie** Szczegóły miejsca realizacji usługi:	Warunki logistyczne: