Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

441 ocen

Techniki hackingu i cyberprzestępczości - PTH, eskalacje i obejście zabezpieczeń - poziom 4

Numer usługi 2026/01/20/17164/3270882

zdalna w czasie rzeczywistym

Usługa szkoleniowa

21 h

18.02.2026 do 20.02.2026

6 014,70 PLN brutto

4 890,00 PLN netto

286,41 PLN brutto/h

232,86 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Wychodząc naprzeciw najbardziej wymagającym klientom, którzy oczekują sporej dawki wiedzy, adrenaliny i możliwości przetestowania swoich umiejętności, udostępniona zostaje piąta część cyklu szkoleń nt. hackingu. Główny obszar, na którym się koncentruje to PTH, eskalacja uprawnień w systemach Linux i Windows oraz szeroko rozumiane obejście zabezpieczeń.** Wymagania: • Znajomość podstaw Linuxa, działania sieci, zasady działania systemów • Wiedza ze szkoleń **Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1** oraz **Techniki hackingu i cyberprzestępczości - Systemy i usługi sieciowe - poziom 3** - to absolutne minimum! Jeżeli brałeś udział w całym cyklu szkoleń, jesteś idealnie przygotowany do przygody z najnowszą porcją wiedzy.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	09-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
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

Nabycie umiejętności pozyskiwania haseł i tokenów z pamięci RAM, obejście ograniczeń powłoki w systemie Linux oraz poznanie sposobów na deszyfrację haseł w systemach Windows. System Android również nie zostanie przez nas pominięty. Dodatkowo zajmiemy się hakowaniem wirtualnych maszyn z poziomu gospodarza. Czyli jak włamując się na komputer utrzymujący wirtualizację włamać się do zasobów wirtualnego systemu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi wykrywać luki i przeprowadzać zaawansowany rekonesans oraz analizę informacji o systemie i jego usługach.	W warunkach praktycznych laboratoriów uczestnik identyfikuje i dokumentuje podatności systemowe oraz skutecznie wykorzystuje narzędzia do zaawansowanego skanowania i analizy środowiska.	Obserwacja w warunkach symulowanych
Uczestnik umie eskalować uprawnienia w systemach Linux i Windows oraz obejść mechanizmy zabezpieczeń (np. UAC, ograniczenia powłoki).	W symulowanych scenariuszach uczestnik przeprowadza eskalację uprawnień i obejścia zabezpieczeń zgodnie z instrukcją zadania, osiągając dostęp na uprzywilejowanym poziomie.	Obserwacja w warunkach symulowanych
Uczestnik potrafi pozyskiwać hasła i tokeny z pamięci RAM oraz deszyfrować hasła w środowiskach Windows i Android.	Podczas ćwiczeń laboratoryjnych uczestnik wyodrębnia dane uwierzytelniające z pamięci systemowej oraz stosuje techniki deszyfracji haseł z narzędziami zgodnymi z dobrymi praktykami etycznego hackingu.	Obserwacja w warunkach symulowanych
Uczestnik umie realizować kompleksowe scenariusze ataku, łącząc poznane techniki eskalacji i obejścia zabezpieczeń do uzyskania dostępu do zasobów systemu.	Uczestnik poprawnie planuje i realizuje wieloetapowy scenariusz ataku w środowisku testowym, skutecznie łącząc co najmniej dwie techniki eskalacji uprawnień i obejścia zabezpieczeń, co potwierdza uzyskaniem nieautoryzowanego dostępu do wskazanych zasobów systemu oraz udokumentowaniem przebiegu działań.	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

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

1. Fingerprinting Internetu
2. Analiza szczegółowych informacji na temat firmy, osoby itp.
3. Raportowanie w NMAP-ie
4. Automatyzacja - zmiany wersji pythona napotrzeby określonych ataków
5. Tajemnice Respondera
6. CME - „szwajcarski scyzoryk” w analizach poeksploatacyjnych
7. Pozyskiwanie tokenów i haseł z pamięci RAM
8. Remote Code Execution w systemachWindows
9. Sposoby na poznanie haseł w systemach
10. Windows - Password Dumping
11. Eskalacja uprawnień w systemie Linux
12. Eskalacja w systemie Windows - Bypass UAC
13. Eskalacja uprawnień z wykorzystaniem perl-a
14. Obejście ograniczeń powłoki w systemie Linux
15. Scenariusze uzyskania uprawnień root
16. Podstawy hakowania systemu Android
17. Hakowanie maszyn wirtualnych z poziomu gospodarza
18. Hakowanie serwera Jenkins
19. Hacking Oracle GlassFish - Code Execution
20. Hacking Elasticsearch
21. Ukrywanie payloadow (zdjęcia, wizytówki)
22. Audyty bezpieczeństwa systemów Windows
23. Scenariusz ataku na system informatyczny - 1
24. Scenariusz ataku na system informatyczny – 2

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	6 014,70 PLN
Koszt przypadający na 1 uczestnika netto	4 890,00 PLN
Koszt osobogodziny brutto	286,41 PLN
Koszt osobogodziny netto	232,86 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Armand Pajor

Doświadczenie zawodowe: Trener IT, prowadzący szkolenia w Dagma Szkolenia IT od początku 2023 roku. Wdrożeniowiec i analityk cyberbezpieczeństwa sieci. Prowadzący autorskie szkolenie firmy FORSEC z zakresu Technik hackingu oraz Cyberbezpieczeństwa sieci (Lan Security Analyst) i systemów operacyjnych (OS Security Analyst)
Uzyskane certyfikacje: ITIL Foundation Certificate in IT Service Management, Corporate Readiness Certificate - Information Security Management, Corporate Readiness Certificate - Troubleshooting
Specjalizacja: Sieci komputerowe, Cyberbezpieczeństwo, Network Traffic Analysis, Cyber Threat Hunting (CTH), C#, Python, Java
Wykształcenie: wyższe, Politechnika Krakowska, magister Informatyki.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma:

- materiały dydaktyczne w formie elektronicznej (ebook, do którego dostęp zostanie udostępniony na adres e-mail uczestnika)
- dostęp do środowiska wirtualnego, wysyłany na adres e-mail uczestnika

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

Informacje dodatkowe

Informacje organizacyjne:

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.

- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Szkolenia IT

Warunki techniczne

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl

Kontakt

Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl
Telefon (+48) 327 931 015