Możliwość dofinansowania

NTG.pl Sp. z o.o.

4,4 / 5

5 544 oceny

Szkolenie: Ethical Hacking - poziom średniozaawansowany

Numer usługi 2025/08/29/5395/2971064

1 600,00 PLN brutto
1 600,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
11.12.2025 do 12.12.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Zachodniopomorskie Bony Szkoleniowe, Małopolski Pociąg do kariery
Grupa docelowa usługi	Szkolenie Ethical Hacking – poziom średniozaawansowany jest przeznaczone dla osób, które posiadają podstawową wiedzę z zakresu cyberbezpieczeństwa i chcą rozwinąć umiejętności w praktycznym testowaniu zabezpieczeń. W szczególności szkolenie jest skierowane do: • administratorów sieci i systemów, którzy chcą lepiej chronić swoją infrastrukturę IT, • początkujących pentesterów, szukających praktycznych umiejętności i doświadczenia, • studentów kierunków informatycznych, zainteresowanych bezpieczeństwem IT, • pasjonatów cyberbezpieczeństwa, którzy chcą pogłębić swoją wiedzę w zakresie testów penetracyjnych i ataków na usługi sieciowe oraz aplikacje webowe. **Usługa adresowana również do uczestników projektów: Kierunek Rozwój, Małopolski Pociąg do Kariery, Zachodniopomorskie Bony Szkoleniowe oraz innych programów dofinansowanych.**
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	08-12-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do poznania podstawowych luk w aplikacjach webowych (SQLi, XSS), odpowiedniego wykorzystania narzędzie: Nmap, Burp Suite, Hydra oraz rozwinięcia umiejętności w obszarze testów bezpieczeństwa. Szkolenie pozwoli uczestnikom poznać, jak wygląda atak na podatne usługi sieciowe oraz aplikacje webowe, a także jak je identyfikować i wykorzystywać w środowisku testowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna nmap, podstawowe przełączniki, charakteryzuje enum4linux.	Uczestnik określa zasady wykonania poprawnego skanu, interpretacji wyniku, enumeracji SMB.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik określa zasady zalogowania się anonimowo do FTP, pobierania pliku, testu SMB.	Uczestnik identyfikuje zasoby SMB i podatności.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik charakteryzuje Burp Suite, testy SQLi i XSS.umie używać Hydra do brute-force, przechwytywać NTLM w Responderze.	Uczestnik zna możliwości: przechwytuje/modyfikuje żądania w Burp, wykorzystania SQLi (sqlmap), prezentacji XSS PoC. skutecznego łamania hasła.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik określa ścieżkę ataku, wybiera rekomendacje.	Uczestnik wie jak formułować rekomendacje, przygotować raport końcowy.	Test teoretyczny z wynikiem generowanym automatycznie

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

Szkolenie realizowane w godzinach dydaktycznych (przerwy nie wliczają się w czas trwania usługi)

.

📘 Jak wygląda szkolenie?

Szkolenie prowadzone jest w sposób uporządkowany i praktyczny - składa się z trzech etapów:

- Wprowadzenie teoretyczne
- Ćwiczenia wspólne z trenerem – wykonujemy zadania krok po kroku, ucząc się na konkretnych przykładach.
- Zadania do samodzielnego wykonania – utrwalenie wiedzy.

🤝 Opieka poszkoleniowa

Po zakończeniu szkolenia zapewniamy pełną opiekę poszkoleniową:

- kontakt z trenerem
- wsparcie techniczne i merytoryczne po szkoleniu
- dodatkowe materiały i wskazówki, które pomogą wracać do kluczowych zagadnień.

✅ Program szkolenia:

Moduł 1: Skanowanie i rekonesans:

- Użycie narzędzia nmap
- Podstawowe przełączniki skanowania
- enum4linux i podstawowa enumeracja SMB

Moduł 2: Ataki na usługi sieciowe:

- FTP: logowanie anonimowe, pobieranie plików z użyciem narzędzi w Kali
- SMB: zasoby współdzielone, testowanie znanych luk

Moduł 3: Ataki na aplikacje webowe:

- Poznanie i nauka zaawansowanego użycia narzędzia Burp Suite
- SQL Injection: testowanie ręczne oraz użycie sqlmap
- XSS: reflected i stored, identyfikacja podatnych pól formularzy

Moduł 4: Uwierzytelnianie i hasła:

- Brute-force z użyciem Hydra w Kali
- Przechwytywanie NTLM z wykorzystaniem Respondera w Kali

Moduł 5: Podsumowanie i dobre praktyki:

- Jak uczyć się omawiając przykładowe ścieżki ataków
- Jak odpowiednio dobrać rekomendacje do znalezionych podatności
- Jak stworzyć krótki raport z testu penetracyjnego

Test z wynikiem generowaynym automatycznie.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Moduł 1: Skanowanie i rekonesans - teoria	Daniel Gawryś	11-12-2025	09:00	10:30	01:30
2 z 15 Przerwa - nie wlicza się czas trwania usługi	Daniel Gawryś	11-12-2025	10:30	10:45	00:15
3 z 15 Moduł 1: Skanowanie i rekonesans - praktyka	Daniel Gawryś	11-12-2025	10:45	12:15	01:30
4 z 15 Przerwa - nie wlicza się czas trwania usługi	Daniel Gawryś	11-12-2025	12:15	12:30	00:15
5 z 15 Moduł 2: Ataki na usługi sieciowe - teoria	Daniel Gawryś	11-12-2025	12:30	14:00	01:30
6 z 15 Przerwa - nie wlicza się czas trwania usługi	Daniel Gawryś	11-12-2025	14:00	14:15	00:15
7 z 15 Moduł 2: Ataki na usługi sieciowe - praktyka	Daniel Gawryś	11-12-2025	14:15	15:45	01:30
8 z 15 Moduł 3: Ataki na aplikacje webowe - teoria	Daniel Gawryś	12-12-2025	09:00	10:30	01:30
9 z 15 Przerwa - nie wlicza sie w czas trwania usługi	Daniel Gawryś	12-12-2025	10:30	10:45	00:15
10 z 15 Moduł 3: Ataki na aplikacje webowe - praktyka	Daniel Gawryś	12-12-2025	10:45	12:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 15 Przerwa - nie wlicza sie w czas trwania usługi	Daniel Gawryś	12-12-2025	12:15	12:30	00:15
12 z 15 Moduł 4: Uwierzytelnianie i hasła;	Daniel Gawryś	12-12-2025	12:30	14:00	01:30
13 z 15 Przerwa - nie wlicza się w czas trwania	Daniel Gawryś	12-12-2025	14:00	14:15	00:15
14 z 15 Moduł 5: Podsumowanie i dobre praktyki	Daniel Gawryś	12-12-2025	14:15	15:30	01:15
15 z 15 Test z wynikiem generowanym automatycznie	Daniel Gawryś	12-12-2025	15:30	15:45	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 600,00 PLN
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Gawryś

Entuzjasta cyberbezpieczeństwa z praktycznym doświadczeniem w przeprowadzaniu szkoleń, testów penetracyjnych, analizie podatności i zabezpieczaniu środowisk IT(Trener posiada

doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR)
Posiadam certyfikaty eCPPT, CPTS
(od HTB), Cisco Junior Cybersecurity Analyst i Cisco Certified Ethical Hacker. Tworzy własne narzędzia w Pythonie i Bashu, aktywnie uczestniczę w CTF-ach oraz rozwija umiejętności w homelabach zgodnie z metodykami OWASP i MITRE ATT&CK. Prowadzący posiada wiedzę i doświadczenie z zakresu zaawansowanych technik hackingu oraz przeciwdziałania atakom. Posiada doświadczenie zdobyte w oparciu o przeprowadzone pentest infrastruktury sieci szkolnej, sieci w placówkach państwowych oraz stron internetowych różnych firm.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autorskie materiały szkoleniowe w wersji elektronicznej.

Warunki uczestnictwa

Uczestnik powinien posiadać wiedzę z obszarów:

- Znajomość podstaw TCP/IP i terminala
- System z Burp, nmap i Hydra (np. Kali Linux)

Informacje dodatkowe

Po ukończeniu szkolenia uczestnik otrzymuje certyfikat potwierdzający zdobyte umiejętności.

Jak skorzystać z usług dofinansowanych?

- Krok 1: Założenie konta indywidualnego/instytucjonalnego w Bazie Usług Rozwojowych.
- Krok 2: Złożenie wniosku do Operatora, który rozdziela środki w Twoim województwie.
- Krok 3: Uzyskanie dofinasowania.
- Krok 4: Zapisanie na szkolenie poprzez platformę BUR.

Podczas szkoleń istnieje możliwość przeprowadzenia kontroli/audytu usługi przez osoby do tego upoważnione przez PARP oraz nagrywania usługi.

Dlaczego wybrać firmę NTG Sp. z o.o.?

- Realizujemy szkolenia od 2002 roku.
- Mamy wyspecjalizowaną kadrę szkoleniową.
- Przeprowadzimy Ciebie przez cały proces pozyskania dofinansowania.
- Bezpłatnie pomożemy w uzyskaniu dofinansowania.
- Zaproponujemy szkolenia dopasowane do potrzeb Twojej firmy.
- Dostarczymy dokumentację szkoleniową, niezbędną do rozliczenia.
- Odpowiemy na wszystkie Twoje pytania.

Warunki techniczne

Zalecamy korzystanie z dodatkowego monitora, aby móc swobodnie wykonywać ćwiczenia wraz z trenerem.

Szkolenie będzie realizowane za pośrednictwem aplikacji Microsoft Teams (nie jest wymagana instalacja aplikacji). Link do spotkania można otworzyć za pomocą przeglądarki i jest aktywny podczas trwania usługi.

Do poprawnego udziału w usłudze uczestnik powinien posiadać komputer z kamerą, mikrofonem, dostępem do Internetu; szybkością pobierania i przesyłania 500 kb/s; aktualną wersje przeglądarki Microsoft Edge, Internet Explorer, Safari lub Chrome. Zalecamy posiadanie systemu operacyjnego Windows 10 oraz min. 2 GB RAM pamięci.

Kontakt

NTG.pl Sp. z o.o.

E-mail ntg@ntg.edu.pl

Telefon (+48) 609 009 742