Możliwość dofinansowania

NTG.pl Sp. z o.o.

4,4 / 5

5 553 oceny

Szkolenie: Ethical Hacking - Poziom Zaawansowany

Numer usługi 2025/10/21/5395/3094955

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

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
09.12.2025 do 11.12.2025

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 skierowane jest do osób, które mają już doświadczenie w testach penetracyjnych i chcą rozwinąć swoje umiejętności w zakresie bardziej złożonych scenariuszy ataku, w tym ataków na środowiska Active Directory oraz łańcuchowania podatności. Idealne dla: • pentesterów z podstawowym doświadczeniem, • specjalistów ds. cyberbezpieczeństwa, • administratorów chcących zrozumieć wektory ataku na infrastrukturę AD, • osób przygotowujących się do certyfikacji OSCP/OSWE/CRTP. Usługa adresowana również do uczestników Projektów: Kierunek Rozwój, Małopolski Pociąg do Kariery, Zachodniopomorskie Bony Szkoleniowe oraz uczestników innych programów dofinansowanych.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	04-12-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do wykorzystania pojedynczych podatności, łączenia ich w realistyczne scenariusze ataku, prowadzące do pełnego przejęcia środowiska. Obejmuje również techniki SSRF i SSTI często wykorzystywane w atakach na aplikacje webowe oraz ścieżkę lateral movement wewnątrz sieci korporacyjnej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wykonuje zaawansowany rekonesans sieciowy i fingerprinting usług (Nmap, masscan, TLS/HTTP, WAF).	Uczestnik stosuje praktyczne zadania modułowe: wykonuje skanu 100+ hostów, dowody fingerprintingu i działający tunel pivot (ocena punktowa; próg modułu ≥70%).	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wie jak zidentyfikować i bezpiecznie zweryfikować krytyczne podatności webowe (SSRF, SSTI) oraz zbudować PoC.	Uczestnik określa działający, kontrolowany dowód (SSRF/SSTI) z dokumentacją komend i artefaktów (punktacja za wykrycie i bezpieczne PoC).	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przeprowadzi pivoting do sieci wewnętrznej (SSH tunnel, SOCKS, Chisel) i potwierdzi dostęp do zasobów wewnętrznych.	Uczestnik zna AD i Kerberos: dostarczenie listy kont/SPN, zrzutów BloodHound i wyników Kerberoast/AS-REP (dowody + analiza).	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik enumeruje Active Directory i analizuje ścieżki ataku przy użyciu BloodHound; wykona Kerberoasting/AS-REP Roasting.	Uczestnik wie jak wykorzystać Lateral & LPE: udokumentowane przejście na kolejny host i eskalacja uprawnień z PoC (zrzuty/logi).	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.

📘 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: Zaawansowany rekonesans i pivoting:

- Zaawansowane skanowanie Nmap, masscan
- Fingerprinting systemów i usług (HTTP headers, TLS fingerprints, WAF)
- Techniki pivotingu (SSH tunneling, Chisel, socks proxies)

Moduł 2: Zaawansowane podatności webowe:

- SSRF – rozpoznanie i wykorzystanie, dostęp do zasobów wewnętrznych (AWS metadata, GCP, lokalne aplikacje)
- SSTI – identyfikacja silników szablonów (Jinja2, Twig), wykonanie RCE
- Wprowadzenie do łańcuchowania podatności (e.g., SSRF + RCE → reverse shell)

Moduł 3: Wprowadzenie do ataków na Active Directory:

- Enumeracja AD (LDAP, Kerberos, SMB)
- BloodHound – analiza ścieżek ataku
- AS-REP Roasting, Kerberoasting
- Ataki na konta serwisowe, przechwytywanie biletów TGT, użycie mimikatz

Moduł 4: Lateral movement i privilege escalation:

- Pass-the-Hash, Overpass-the-Hash, Pass-the-Ticket
- Abuse Delegation (Unconstrained, Constrained)
- Local Privilege Escalation (winPEAS, SharpUp)
- Wstęp do Domain Persistence (Golden Ticket, DSRM)

Moduł 5: Scenariusz: Pentest end-to-end:

- Początek z zewnątrz (enumeracja hostów, usług webowych, brute-force)
- Wykorzystanie SSRF → pivot do sieci wewnętrznej
- Eksploatacja hostów → zdobycie footholda
- Ruch lateralny do DC, przejęcie domeny
- Raportowanie i ścieżka ataku

Moduł 6: Raportowanie i obrona:

- Jak pisać dobry raport pentesterski
- Mapowanie rekomendacji do ryzyk
- Wskazówki dot. zabezpieczenia AD

Zakończenie:

- Symulacja Red Team / mini CTF: 2 godziny na przejęcie domeny
- Przekazanie flagi: kontrola konta Domain Admin
- Omówienie ścieżki ataku i podsumowanie szkolenia

Test z wynikiem generowanym automatycznie.

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Moduł 1: Zaawansowany rekonesans i pivoting; Moduł 2: Zaawansowane podatności webowe	Daniel Gawryś	09-12-2025	09:00	15:00	06:00
2 z 4 Moduł 3: Wprowadzenie do ataków na Active Directory; Moduł 4: Lateral movement i privilege escalation	Daniel Gawryś	10-12-2025	09:00	15:00	06:00
3 z 4 Moduł 5: Scenariusz: Pentest end-to-end; Moduł 6: Raportowanie i obrona	Daniel Gawryś	11-12-2025	09:00	14:45	05:45
4 z 4 Test z wynikiem generowanym automatycznie	Daniel Gawryś	11-12-2025	14:45	15:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 400,00 PLN

Koszt przypadający na 1 uczestnika netto	2 400,00 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 testów penetracyjnych, analizie podatności i zabezpieczaniu środowisk IT. 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. Trener posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autorskie materiały szkoleniowe w wersji elektronicznej.

Warunki uczestnictwa

- Znajomość podstaw pentestów (Nmap, Burp, SQLi, XSS).
- Znajomość podstaw działania AD (LDAP, Kerberos, NTLM).
- System z Kali Linux lub Parrot OS (z dostępem do sieci labowej).

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