Możliwość dofinansowania

"LUGA" AGNIESZKA GLIŃSKA

4,9 / 5

1 274 oceny

Ataki i ochrona Active Directory

Numer usługi 2026/04/20/7321/3501100

4 305,00 PLN brutto
3 500,00 PLN netto
107,63 PLN brutto/h
87,50 PLN netto/h
261,33 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
40:00 h
15.06.2026 do 19.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Regionalny Fundusz Szkoleniowy II, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie skierowane jest do osób posiadających podstawową wiedzę z zakresu administracji systemami Windows oraz sieci komputerowych, w szczególności: • administratorów systemów Windows i Active Directory, • specjalistów ds. bezpieczeństwa IT (SOC, Blue Team), • pentesterów i audytorów bezpieczeństwa, • osób odpowiedzialnych za reagowanie na incydenty bezpieczeństwa. Uczestnik powinien posiadać przynajmniej podstawowe doświadczenie w pracy z systemami Windows oraz znajomość podstawowych zagadnień sieciowych i bezpieczeństwa IT.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	14-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do samodzielnego identyfikowania podatności w środowiskach Windows i Active Directory, przeprowadzania testów penetracyjnych oraz analizy incydentów.Uczestnik zdobędzie umiejętności w zakresie:rekonesansu i enumeracji sieci oraz systemów, przeprowadzania ataków na Active Directory(w tym eskalacji uprawnień i lateral movement),wykorzystywania technik m.in.Pass-the-Hash, Kerberoasting czy SMB Relay, zabezpieczania środowisk Windows przed współczesnymi zagrożeniami

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza rekonesans i enumerację środowiska Windows oraz sieci	identyfikuje aktywne hosty w sieci z wykorzystaniem narzędzi skanujących,	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje usługi i otwarte porty na wskazanych systemach,	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje strukturę domeny i wskazuje kluczowe elementy środowiska Active Directory,	Test teoretyczny z wynikiem generowanym automatycznie
	dokumentuje wyniki rekonesansu w uporządkowanej formie.	Test teoretyczny z wynikiem generowanym automatycznie
Wykonuje ataki na środowisko Active Directory w warunkach laboratoryjnych	przeprowadza atak LLMNR Poisoning i przechwytuje dane uwierzytelniające,	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje przechwycone hashe do dalszych działań (np. łamanie haseł),	Test teoretyczny z wynikiem generowanym automatycznie
	realizuje scenariusz SMB Relay lub Pass-the-Hash,	Test teoretyczny z wynikiem generowanym automatycznie
	uzyskuje dostęp do systemu (shell access) zgodnie ze scenariuszem zadania.	Test teoretyczny z wynikiem generowanym automatycznie
Realizuje działania posteksploitacyjne w środowisku Windows	przeprowadza eskalację uprawnień w systemie,	Test teoretyczny z wynikiem generowanym automatycznie
	wykonuje lateral movement pomiędzy systemami w sieci,	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje narzędzia (np. Mimikatz) do pozyskiwania danych uwierzytelniających,	Test teoretyczny z wynikiem generowanym automatycznie
	realizuje scenariusze Kerberoasting lub Golden Ticket zgodnie z instrukcją.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje mechanizmy zabezpieczeń środowiska Windows	konfiguruje podstawowe mechanizmy ochrony (np. LAPS, Credential Guard),	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera odpowiednie zabezpieczenia do zidentyfikowanych zagrożeń,	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje skuteczność zastosowanych zabezpieczeń,	Test teoretyczny z wynikiem generowanym automatycznie
	uzasadnia wybór konkretnych mechanizmów ochronnych.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie „Windows Security and Forensic – bezpieczeństwo systemów Windows, testy penetracyjne i analiza śledcza” jest dostosowane do potrzeb administratorów systemów Windows, specjalistów bezpieczeństwa IT oraz pentesterów.

Program obejmuje zagadnienia związane z bezpieczeństwem systemów Windows, atakami na Active Directory, technikami posteksploitacyjnymi oraz informatyką śledczą.

Szkolenie realizowane jest w formie **warsztatowej (laboratoria w chmurze)**, umożliwiającej uczestnikom wykonywanie ćwiczeń praktycznych w środowisku symulowanym.

Warunki organizacyjne

- szkolenie realizowane w formie online (rozmowa na żywo),

- każdy uczestnik pracuje na **indywidualnym środowisku laboratoryjnym w chmurze**,
- maksymalna liczba uczestników: zgodnie z limitem miejsc (kameralne grupy),
- uczestnicy otrzymują materiały szkoleniowe oraz dostęp do laboratoriów,
- szkolenie prowadzone przez certyfikowanego trenera (MCSE, MCT).

Czas trwania

- 5 dni (25–29.05.2026)
- łącznie: **40 godzin dydaktycznych** (1 godz. dydaktyczna = 45 min)

Podział godzin

- zajęcia teoretyczne: **12 godzin**
- zajęcia praktyczne (laboratoria): **28 godzin**

Przerwy

- przerwy są wliczone w czas szkolenia,
- przewiduje się przerwy krótkie (ok. 5–10 min) oraz jedną dłuższą przerwę dziennie.

Rekonesans i enumeracja

- Omówienie fundamentów Active Directory
- Model Cyber-Kill chain
- Skanowanie i wykrywane hostów
- Wykrywanie domen

Ataki Active Directory (faza wstępna)

- LLMNR Poisoning
- Przechwytywanie NTLMv2 Hash
- Łamanie haseł z wykorzystaniem Hashcat
- SMB Relay Attacks
- Zdobywanie Shell Access
- Credential harvesting z domeną i bez domeny
- Ataki lokalne i ataki zdalne

Atakowanie Active Directory faza posteksploitacji

- Uprawnienia i przywileje w Windows i Active Directory Eskalacja uprawnień / przywilejów
- Lateral Movement
- Pass the Hash / Password
- netexec
- Pass the Password Attacks
- Pass the Hash Attacks
- Token Impersonation
- Kerberoasting
- GPP Password Attacks
- Mimikatz
- PetitPotam, PrinterBug, DFSCoerce
- Skeleton Key, DCShadow, AdminSDHolder
- Golden Ticket Attacks

Ochrona przed atakami

- Tiering Active Directory
- Ochrona przed pass the hash
- Ochrona LSA
- Credential Guard
- Application Whitelisting
- LAPS / Windows LAPS
- MSA ii gMSAAuthentication Silos / Authentication Policies

Ataki Active Directory Certificate Services

- Komponenty AD CS
- Enumeracja ADCS
- Wykrywanie podatnych szablonów
- Klasy podatności ESC1–ESC13
- Ataki relay z wykorzystaniem AD CS
- Zabezpieczanie AD CS

Wykrywanie ataków z wykorzystaniem SIEM

- Metody wykrywania
- Wykrywanie ataków
- Thread Hunting
- Analiza logów SIEM

Harmonogram

Liczba pozycji harmonogramu: 35

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 35 Rekonesans i enumeracja	Rafał Decyk	15-06-2026	09:00	10:30	01:30
2 z 35 Przerwa	Rafał Decyk	15-06-2026	10:30	10:40	00:10
3 z 35 Rekonesans i enumeracja	Rafał Decyk	15-06-2026	10:40	12:10	01:30
4 z 35 Przerwa	Rafał Decyk	15-06-2026	12:10	12:40	00:30
5 z 35 Ataki Active Directory (faza wstępna)	Rafał Decyk	15-06-2026	12:40	14:10	01:30
6 z 35 Przerwa	Rafał Decyk	15-06-2026	14:10	14:20	00:10
7 z 35 Ataki Active Directory (faza wstępna)	Rafał Decyk	15-06-2026	14:20	15:00	00:40
8 z 35 Atakowanie Active Directory faza posteksploitacji	Rafał Decyk	16-06-2026	09:00	10:30	01:30
9 z 35 Przerwa	Rafał Decyk	16-06-2026	10:30	10:40	00:10

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 35 Atakowanie Active Directory faza posteksploitacji	Rafał Decyk	16-06-2026	10:40	12:10	01:30
11 z 35 Przerwa	Rafał Decyk	16-06-2026	12:10	12:40	00:30
12 z 35 Atakowanie Active Directory faza posteksploitacji	Rafał Decyk	16-06-2026	12:40	14:10	01:30
13 z 35 Przerwa	Rafał Decyk	16-06-2026	14:10	14:20	00:10
14 z 35 Atakowanie Active Directory faza posteksploitacji	Rafał Decyk	16-06-2026	14:20	15:00	00:40
15 z 35 Ochrona przed atakami	Rafał Decyk	17-06-2026	09:00	10:30	01:30
16 z 35 Przerwa	Rafał Decyk	17-06-2026	10:30	10:40	00:10
17 z 35 Ochrona przed atakami	Rafał Decyk	17-06-2026	10:40	12:10	01:30
18 z 35 Przerwa	Rafał Decyk	17-06-2026	12:10	12:40	00:30
19 z 35 Ochrona przed atakami	Rafał Decyk	17-06-2026	12:40	14:10	01:30
20 z 35 Przerwa	Rafał Decyk	17-06-2026	14:10	14:20	00:10
21 z 35 Ochrona przed atakami	Rafał Decyk	17-06-2026	14:20	15:00	00:40
22 z 35 Ataki Active Directory Certificate Services	Rafał Decyk	18-06-2026	09:00	10:30	01:30
23 z 35 Przerwa	Rafał Decyk	18-06-2026	10:30	10:40	00:10

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 35 Ataki Active Directory Certificate Services	Rafał Decyk	18-06-2026	10:40	12:10	01:30
25 z 35 Przerwa	Rafał Decyk	18-06-2026	12:10	12:40	00:30
26 z 35 Ataki Active Directory Certificate Services	Rafał Decyk	18-06-2026	12:40	14:10	01:30
27 z 35 Przerwa	Rafał Decyk	18-06-2026	14:10	14:20	00:10
28 z 35 Ataki Active Directory Certificate Services	Rafał Decyk	18-06-2026	14:20	15:00	00:40
29 z 35 Wykrywanie ataków z wykorzystaniem SIEM	Rafał Decyk	19-06-2026	09:00	10:30	01:30
30 z 35 Przerwa	Rafał Decyk	19-06-2026	10:30	10:40	00:10
31 z 35 Wykrywanie ataków z wykorzystaniem SIEM	Rafał Decyk	19-06-2026	10:40	12:10	01:30
32 z 35 Przerwa	Rafał Decyk	19-06-2026	12:10	12:40	00:30
33 z 35 Wykrywanie ataków z wykorzystaniem SIEM	Rafał Decyk	19-06-2026	12:40	14:10	01:30
34 z 35 Przerwa	Rafał Decyk	19-06-2026	14:10	14:20	00:10
35 z 35 Walidacja efektów + podsumowanie	Rafał Decyk	19-06-2026	14:20	15:00	00:40

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 305,00 PLN
Koszt przypadający na 1 uczestnika netto	3 500,00 PLN
Koszt osobogodziny brutto	107,63 PLN
Koszt osobogodziny netto	87,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Rafał Decyk

Szkolenie jest prowadzone przez doświadczonego specjalistę w obszarze bezpieczeństwa systemów Microsoft, posiadającego ponad 5-letnie doświadczenie zawodowe w zakresie:
• administracji i zabezpieczania środowisk Windows oraz Active Directory,
• realizacji testów penetracyjnych i audytów bezpieczeństwa,
• wdrażania rozwiązań z zakresu cyberbezpieczeństwa,
• analizy incydentów bezpieczeństwa (SOC / Blue Team / Digital Forensics).
Trener posiada doświadczenie praktyczne zdobyte przy realizacji projektów dla firm i instytucji, obejmujących m.in.:
• wdrożenia i zabezpieczanie środowisk AD,
• testy penetracyjne infrastruktury IT,
• analizę zdarzeń bezpieczeństwa oraz reagowanie na incydenty.

Kwalifikacje i certyfikaty
Trener posiada aktualne kwalifikacje zawodowe, w tym certyfikaty branżowe, np.:
• Microsoft Certified Solutions Expert (MCSE),
• Microsoft Certified Trainer (MCT),
• certyfikaty z obszaru bezpieczeństwa IT i administracji systemami.
Posiada również udokumentowane doświadczenie szkoleniowe w prowadzeniu kursów z zakresu bezpieczeństwa systemów Windows i Active Directory.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

materiały szkoleniowe w pdf

Warunki uczestnictwa

Szkolenie realizowane jest w formie zdalnej w czasie rzeczywistym (online) z wykorzystaniem narzędzi umożliwiających bezpośrednią komunikację uczestników z trenerem.

Sposób realizacji zajęć

Zajęcia prowadzone są w formule:

- **rozmowy na żywo (audio/wideo)**,
- **ćwiczeń praktycznych realizowanych w środowisku laboratoryjnym w chmurze**,
- **współdzielenia ekranu przez trenera i uczestników**,
- **czatu do komunikacji bieżącej**,
- **konsultacji indywidualnych w trakcie zajęć**,
- **zadań praktycznych (scenariusze laboratoryjne)**.

Uczestnicy wykonują zadania samodzielnie pod nadzorem trenera, który na bieżąco monitoruje postępy i udziela wsparcia.

Szkolenie prowadzone jest przy użyciu platformy umożliwiającej kontakt w czasie rzeczywistym (np. ClickMeeting lub równoważnej), zapewniającej:

- transmisję audio-wideo,
- możliwość zadawania pytań na żywo,
- współdzielenie ekranu,
- kontrolę aktywności uczestników.

Warunki techniczne

Uczestnik powinien dysponować:

- komputerem (laptop/PC) z dostępem do Internetu (zalecane stabilne łącze min. 10 Mb/s),
- procesorem min. 2 GHz (zalecany wielordzeniowy),
- minimum 4 GB pamięci RAM (zalecane 8 GB),
- systemem operacyjnym: Windows 10/11, macOS, Linux lub Chrome OS,
- aktualną przeglądarką internetową (Chrome, Edge, Firefox),
- sprawnym mikrofonem i głośnikiem lub zestawem słuchawkowym,
- zalecana kamera internetowa (dla pełnej interakcji z trenerem).

Dodatkowe wymagania

- podstawowa znajomość systemów Windows i zagadnień sieciowych,
- umiejętność obsługi komputera i pracy w środowisku IT,
- gotowość do pracy warsztatowej (wykonywanie ćwiczeń praktycznych).

Kontakt

Agnieszka Glińska

E-mail info@luga.pl

Telefon (+48) 692 547 267