Program kursu

CyberSecurity Engineer

kurs wieczorowy

66 h zajęć z trenerem na żywo

35 h pracy własnej

70% / 30% praktyki / teorii

Postaw na praktykę

O KURSIE

Kurs CyberSecurity Engineer

Broń systemów. Myśl jak atakujący.

Jeśli rozumiesz, jak działają systemy oraz aplikacje, ale chcesz odkryć ich luki i nauczyć się je łatać, to miejsce dla Ciebie. Kurs CyberSecurity Engineer to idealny start dla osób z zapleczem technologicznym, które chcą zdobyć praktyczne narzędzia do testów penetracyjnych i obrony infrastruktury IT przed realnymi zagrożeniami z zewnątrz.

Co będziesz potrafić po kursie?

- Przeprowadzasz testy penetracyjne aplikacji i sieci
- Pracujesz z Kali Linux i Metasploit
- Analizujesz incydenty i hardenujesz systemy
- Przygotowujesz się do egzaminu CPTE (Mile2)

JAK WYGLĄDA NAUKA

Liczba godzin i forma zajęć

Zajęcia odbywają się zależnie od edycji w poniedziałki i środy lub wtorki i czwartki w godzinach 17:30-20:30.

15 h

Prework

szacowany czas na przygotowanie do kursu

66 h

Zajęcia z trenerem

zdalnie na żywo, zakończone certyfikatem

20 h

Praca własna

szacowany czas na pracę indywidualną między zajęciami

Co zbudujesz na kursie — projekt końcowy

Zrealizujesz kompleksowy projekt testów penetracyjnych: od scenariusza, przez wykonanie testów, po przygotowanie raportu.

- ✓ Pełny cykl pentestu: Recon → Scanning → Exploitation → Post-Exploitation → Reporting
- ✓ Tworzenie raportów zgodne ze standardami CPTE/CPEH
- ✓ Realne scenariusze ataków (AD, API)

▷ Nagrania z zajęć

Nagrania wideo z zajęć dostępne przez 6 miesięcy po zakończeniu kursu.

⚙ Narzędzia i technologie

W praktyce opanujesz: GitHub, Wireshark, Kali Linux, Burp Suite, Nmap, Hashcat, VirtualBox, Metasploit, Linux, Windows, OWASP. Zakres opiera się na realnych case studies.

★ Certyfikat

Kurs przygotowuje do certyfikatu CPTE oraz kończy się certyfikatem ukończenia.

AI AI w kursie

Uczysz się korzystać z AI jak nowoczesny specjalista — do przyspieszania pracy, debugowania i analizy — zawsze z weryfikacją wyniku przez człowieka.

PROGRAM KURSU

CyberSecurity Engineer

8 modułów · 66 h

0

MODUŁ 0 · PREWORK

Prework

Wstępny etap kursu, którego celem jest przygotowanie uczestników do efektywnej pracy w środowisku labowym i wyrównanie poziomu technicznego grupy. Krok po kroku konfigurujesz niezbędne narzędzia i własny lab z podatnymi aplikacjami.

ZAKRES MODUŁU

- Instalacja i konfiguracja środowiska wirtualnego (VirtualBox + Extension Pack)
- Uruchamianie maszyn wirtualnych z Kali Linux i Windows
- Instalacja oraz podstawy obsługi narzędzia Wireshark do analizy ruchu sieciowego
- Konfiguracja środowiska labowego z podatnymi aplikacjami (DVWA, Juice Shop)
- Tworzenie i łączenie maszyn w wewnętrznej sieci wirtualnej
- Weryfikacja działania labu (test ping, przechwytywanie pakietów)

1

MODUŁ 1

Wprowadzenie do bezpieczeństwa

Fundament kursu wprowadzający kluczowe pojęcia i zagadnienia związane z cyberbezpieczeństwem. Poznajesz model CIA, najważniejsze terminy, role i ścieżki rozwoju w branży security oraz podstawy modelowania zagrożeń.

ZAKRES MODUŁU

- Model CIA (Confidentiality, Integrity, Availability) – fundament cyberbezpieczeństwa
- Kluczowe pojęcia: exploit, payload, wektory ataku
- Różne rodzaje testowania: black box, white box, grey box
- Znaczenie prawa i etyki w pracy specjalisty security
- Typowe zagrożenia i realne case studies
- Podstawy modelowania zagrożeń (STRIDE, DFD)

2

MODUŁ 2

Podstawy sieci i systemów

Moduł o fundamentach działania sieci komputerowych i systemów operacyjnych. Poznajesz model OSI, protokoły TCP/IP, adresację i subnetting, różnice między Linux a Windows oraz wprowadzenie do technik eskalacji uprawnień.

ZAKRES MODUŁU

- Model OSI i stos TCP/IP
- Protokoły: TCP, UDP, ICMP, DNS
- Podstawy subnettingu
- Narzędzia tcpdump i Wireshark
- Zasady przeprowadzania ataków ARP spoofing, DHCP starvation, MITM
- Różnice między Linux a Windows w kontekście bezpieczeństwa
- Techniki eskalacji uprawnień i narzędzia LinPEAS, WinPEAS, BloodHound

3

MODUŁ 3

Narzędzia i metodyka testów penetracyjnych

Moduł skupiony na metodologii, narzędziach i praktyce testów penetracyjnych. Przechodzisz pełny cykl pentestu – od rekonesansu i skanowania, przez exploitation, aż po post-exploitation i raportowanie, pracując z Nmap, Metasploit, Hashcat czy Burp Suite.

ZAKRES MODUŁU

- Metodyka pentestów (Recon, Scanning, Exploitation, Reporting)
- Sposób działania narzędzia Metasploit i modułów exploitów/payloadów
- Praktyczne exploity (np. EternalBlue)
- Mechanizmy unikania detekcji (AV/IDS/EDR bypass)
- Narzędzia do łamania haseł (John the Ripper, Hashcat)
- Rola Social Engineering (phishing, trojany, SET)
- Ataki wspierane przez AI (AI phishing, deepfake)

MODUŁ 4

4 Bezpieczeństwo aplikacji webowych

Moduł poświęcony bezpieczeństwu aplikacji webowych – obszarowi stanowiącemu największą część pracy pentesterów. Poznajesz OWASP Top 10, narzędzia do testów webowych i API oraz techniki wzmacniania bezpieczeństwa aplikacji (hardening).

ZAKRES MODUŁU

- Najczęstsze podatności webowe (SQLi, XSS, CSRF, SSRF, XXE, RCE)
- Wykorzystanie Burp Suite (proxy, fuzzing, automatyczne skany)
- Enumerowanie katalogów i plików ukrytych (Gobuster, Dirbuster)
- Podstawy bezpieczeństwa API (REST, GraphQL, OpenAPI)
- Testowanie ataków brute force i credential stuffing
- Typowe błędy implementacyjne w JWT i BOLA
- Działanie WAF, walidacja danych, szyfrowanie, security headers

MODUŁ 5

5 Bezpieczeństwo chmurowe i DevSecOps

Moduł wprowadzający w zagadnienia bezpieczeństwa w chmurze i praktyki DevSecOps. Poznajesz modele usług i odpowiedzialności, typowe zagrożenia chmurowe, narzędzia do audytu oraz rolę automatyzacji bezpieczeństwa w cyklu CI/CD.

ZAKRES MODUŁU

- Modele chmurowe (IaaS, PaaS, SaaS)
- Model odpowiedzialności dzielonej (AWS, Azure, GCP)
- Typowe ataki w chmurze (misconfigured S3, klucze dostępu)
- Użycie ScoutSuite i kube-bench przy audycie
- Idea DevSecOps i shift-left security
- Różnice między SAST i DAST oraz narzędzia (SonarQube, OWASP ZAP)
- SBOM i supply chain attacks

6

MODUŁ 6

Cyber Threat Intelligence i nowoczesna obrona

Moduł wprowadzający w zagadnienia CTI i pracy Blue Team. Uczysz się korzystać z narzędzi do analizy zagrożeń, poznajesz ramy MITRE ATT&CK oraz podstawy analizy logów.

ZAKRES MODUŁU

- Podstawy Cyber Threat Intelligence (CTI)
- Korzystanie z VirusTotal, AbuseIPDB, Shodan
- Ramy MITRE ATT&CK
- Sposób działania Blue Team i jego zadania
- Narzędzia do analizy logów (Sysmon, Graylog, ELK)
- Podstawy pracy z EDR (np. CrowdStrike, Defender)

7

MODUŁ 7

Projekty praktyczne i przygotowanie do egzaminu

Ostatni, praktyczny moduł przygotowujący do egzaminu certyfikacyjnego. Realizujesz pełny projekt pentestowy – od rekonesansu po raportowanie – a moduł kończy się powtórką najważniejszych tematów i symulacją egzaminu.

ZAKRES MODUŁU

- Realizacja pełnego projektu pentestowego (Recon → Scanning → Exploitation → Post-Exploitation → Reporting)
- Tworzenie raportów zgodne ze standardami CPTE/CPEH
- Realne scenariusze ataków (AD, API)
- Struktura pytań egzaminacyjnych i sposoby podejścia do testów
- Quizy i analiza pytań egzaminacyjnych
- Wskazówki dotyczące zarządzania czasem i przygotowania do egzaminu
- Dalsze ścieżki rozwoju (OSCP, CISSP, inne certyfikacje)

FORMY FINANSOWANIA

Sfinansuj kurs tak, jak Ci wygodnie

W infoShare Academy oferujemy różne formy sfinansowania kursu — bez względu na to, który pakiet wybierzesz. Sprawdź, która forma jest dla Ciebie najlepsza!

01 Raty PayU 0%

Najszybszy sposób na rozłożenie płatności na niskie, comiesięczne raty. Do wyboru 5, 10 lub 15 rat 0% albo 24, 36, a nawet 50 rat nisko oprocentowanych.

02 Płatność jednorazowa

Płacisz i zaczynasz naukę. Jednorazowa płatność często wiąże się z dużym rabatem — zapytaj o niego nasze konsultantki.

03 Płatność ratalna

Możliwość rozłożenia płatności na wygodne raty wewnątrz Akademii. Skontaktuj się z nami, aby poznać szczegółowy harmonogram płatności.

04 Dofinansowanie z Urzędu Pracy

Warunkiem jest status osoby bezrobotnej oraz gwarancja zatrudnienia od przyszłego pracodawcy. Wniosek składasz osobiście w swoim Urzędzie Pracy.

05 Baza Usług Rozwojowych (BUR)

Nawet do 80% dofinansowania na kursy w infoShare Academy — dla pracowników mikro, małych i średnich firm, osób prowadzących działalność oraz sektora publicznego i NGO.

06 Pożyczki na kształcenie

Nieoprocentowana pożyczka spłacana do 36 miesięcy, finansuje do 100% kosztów (maks. 75 000 zł). Możliwe umorzenie od 25% do 50% kwoty.

07 Krajowy Fundusz Szkoleniowy (KFS)

Inicjatywa ze środków Funduszu Pracy wspierająca pracodawców inwestujących w kształcenie ustawiczne pracowników oraz własne.

INFOSHARE ACADEMY

Stawiamy na jakość

2015
uczymy IT
od tego roku

9970+
przeszkolonych
osób

330+
trenerów
w naszej kadrze

Łączymy kompetencje techniczne z praktyką biznesową, a każdy kurs prowadzą trenerzy pracujący na co dzień w branży. Dzięki temu uczysz się tego, co realnie przydaje się w pracy.

SL

MASZ PYTANIA?

Sylwia Liedtke

Doradczyni ds. kursów

+48 730 822 825 · sylwia.liedtke@infoshareacademy.com