

Szkolenie: CompTIA CompTIA PenTest+ Prep Course



DOSTĘPNE TERMINY

| | | |
|------------|-------|---------------------------|
| 2026-06-15 | 5 dni | Warszawa / Wirtualna sala |
| 2026-07-13 | 5 dni | Warszawa / Wirtualna sala |
| 2026-08-10 | 5 dni | Kraków / Wirtualna sala |
| 2026-09-14 | 5 dni | Warszawa / Wirtualna sala |
| 2026-10-12 | 5 dni | Kraków / Wirtualna sala |
| 2026-11-16 | 5 dni | Warszawa / Wirtualna sala |
| 2026-12-14 | 5 dni | Kraków / Wirtualna sala |

Cel szkolenia:

Szkolenie **CompTIA PenTest+** potwierdza kompetencje w zakresie identyfikacji, mitygacji oraz raportowania podatności systemowych w pełnym cyklu testów penetracyjnych. Program kładzie silny nacisk na praktykę, obejmując zróżnicowane powierzchnie ataku - od rozwiązań chmurowych i aplikacji webowych, po interfejsy API oraz urządzenia IoT. Uczestnicy rozwijają umiejętności niezbędne w pracy **pentestera** i konsultanta ds. bezpieczeństwa, doskonaląc techniki zarządzania podatnościami, weryfikacji wyników oraz zaawansowane działania poeksplotacyjne, takie jak **post-exploitation** i poruszanie się lateralne wewnątrz infrastruktury.

Jakie umiejętności rozwiniiesz:

- Nauczysz się planować i określać zakres testów penetracyjnych zgodnie z wymogami prawnymi i etycznymi oraz przygotowywać raporty z rekomendacjami wspierającymi procesy zarządzania.
- Będziesz prowadzić rozpoznanie aktywne i pasywne, zbierać informacje oraz enumerować systemy w celu skutecznego wykrywania potencjalnych podatności.
- Wykonasz profesjonalne skany podatności, przeanalizujesz ich wyniki i zweryfikujesz ustalenia, aby precyzyjnie potwierdzić i opisać słabości bezpieczeństwa.
- Przećwiczysz ataki na sieć, hosty, aplikacje webowe i środowiska chmurowe, dobierając odpowiednie narzędzia i techniki do weryfikacji skuteczności zabezpieczeń.
- Poznasz techniki post-exploitation, w tym utrzymanie dostępu oraz poruszanie się lateralne, a także nauczysz się dokumentować ustalenia w sposób wspierający proces usuwania podatności.

Role zawodowe, którym przydadzą się umiejętności PenTest+:

- Pentester
- Analityk cyberbezpieczeństwa
- Konsultant ds. bezpieczeństwa
- Specjalista ds. testów penetracyjnych w środowiskach chmurowych
- Pentester aplikacji webowych
- Specjalista ds. bezpieczeństwa chmury
- Specjalista ds. sieci i bezpieczeństwa

Każdy uczestnik autoryzowanego szkolenia CompTIA PenTest+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA PenTest+ (PT0-003).

Plan szkolenia:

- Testy penetracyjne - zanim zaczniesz
 - Metodyka profesjonalnych testów penetracyjnych: od kodeksu etycznego po raport końcowy
 - Czym są testy penetracyjne?
 - Aspekty regulacyjne i etyczne: standardy postępowania w audytach ofensywnych
 - Znaczenie dokumentacji - przykłady i dobre praktyki
 - Zakres testów i autoryzacja działań
 - Przegląd raportu z testu penetracyjnego
 - Laboratorium: poznanie środowiska laboratoryjnego
 - Interakcje z klientem: kluczowe aspekty komunikacji w procesie testów penetracyjnych
 - Standardy współpracy i komunikacji w procesie testów penetracyjnych
 - Struktura zespołu: role i zakres odpowiedzialności w projektach pentestowych
 - Komunikacja z klientem i członkami zespołu
 - Przegląd partnerski jako mechanizm kontroli merytorycznej w audytach bezpieczeństwa
 - Uzgodnienie oczekiwań z interesariuszami
 - Analiza przyczyn źródłowych
 - Ścieżka eskalacji
 - Bezpieczna dystrybucja wyników testów
 - Metodyka prezentowania ryzyka: kategoryzacja dotkliwości i analiza wpływu
 - Przełożenie podatności technicznych na ryzyko biznesowe i ciągłość operacyjną
 - Formalna akceptacja klienta i proces zatwierdzania raportu z testów

- Frameworki i metodyki testów penetracyjnych: standardy branżowe i podejścia procesowe
 - Przegląd standardów branżowych: od frameworków technicznych po metodyki procesowe
 - Open-Source Security Testing Methodology Manual
 - Council of Registered Ethical Security Testers
 - Penetration Testing Execution Standard
 - MITRE ATT&CK
 - OWASP Top 10
 - OWASP Mobile Application Security Verification Standard
 - Purdue Model
 - Frameworki modelowania zagrożeń
- Wprowadzenie do automatyzacji zadań przy użyciu kodu w testach penetracyjnych
 - Języki skryptowe
 - Powłoka Bash i skrypty Bash
 - Python
 - PowerShell
 - Wykorzystanie bibliotek, funkcji i klas
 - Konstrukcje logiczne
 - Tworzenie konstrukcji logicznych
- Działania przed rozpoczęciem testów penetracyjnych
 - Definiowanie zakresu
 - Przegląd wymogów prawnych i technicznych standardów w audytach ofensywnych
 - Zasady zaangażowania i operacyjne aspekty prowadzenia testów w infrastrukturze
 - Przegląd standardowych typów porozumień zawieranych przed rozpoczęciem audytu
 - Kryteria i proces wyboru celów w ramach zdefiniowanego zakresu testów
 - Porównanie typów ocen
 - Przegląd typów ocen
 - Oceny aplikacji i usług webowych
 - Oceny sieci
 - Ćwiczenie: ocena uwarunkowań środowiskowych
 - Oceny urządzeń mobilnych
 - Oceny środowisk chmurowych
 - Oceny sieci bezprzewodowych
 - IoT a testy penetracyjne
 - IT vs. OT

- Zastosowanie modelu współdzielonej odpowiedzialności w rozwiązaniach chmurowych
 - Przegląd modelu współdzielonej odpowiedzialności
 - Odpowiedzialności dostawcy usługi hostingowej
 - Odpowiedzialności klienta
 - Odpowiedzialności pentestera
 - Odpowiedzialności stron trzecich
- Identyfikacja aspektów prawnych i etycznych
 - Formalne listy autoryzacyjne jako podstawa prawna do działań w infrastrukturze klienta
 - Realizacja ustawowych i regulacyjnych obowiązków raportowych w testach
 - Analiza zagrożeń dla pentestera podczas realizacji działań ofensywnych
 - Formalny zapis ustaleń wstępnych i przygotowań do audytu bezpieczeństwa
- Enumeracja i rozpoznanie
 - Techniki zbierania informacji
 - Rozpoznanie aktywne i pasywne
 - Narzędzia do rozpoznania
 - Wywiad ze źródeł otwartych (OSINT)
 - Wykorzystanie Shodan
 - Listy haseł z wcześniejszych wycieków
 - Rozpoznanie sieci
 - Podstawy skanowania
 - Rozpoznanie z użyciem Nmap
 - Zasady ujawniania informacji o podatnościach i zarządzanie wyciekiem danych
 - Analiza i enumeracja z użyciem wyszukiwarek
 - Metody przechwytywania ruchu sieciowego i analiza danych w transmisji
 - Manipulacja danymi
 - Techniki wykrywania hostów i usług
 - Wyjaśnienie procesu enumeracji jako kluczowej fazy zbierania informacji o celu
 - Wykrywanie hostów
 - Zastosowanie NSE w Nmap
 - Ćwiczenie: użycie skryptów NSE w Nmap
 - Techniki Banner Grabbing i identyfikacja wersji usług sieciowych
 - Enumeracja protokołów
 - Wykrywanie usług na hostach
 - Enumeracja DNS
 - Fingerprinting systemu operacyjnego
 - Enumeracja z użyciem Nmap

- Laboratorium: enumeracja DNS i rozpoznanie
- Enumeracja na potrzeby planowania ataku
 - Mapowanie ścieżek ataku
 - Enumeracja manualna
 - Enumeracja SNMP
 - Dokumentowanie działań enumeracyjnych
 - Ćwiczenie: dokumentowanie działań enumeracyjnych
- Enumeracja wybranych typów zasobów
 - Enumeracja katalogów
 - Enumeracja użytkowników
 - Enumeracja sieci bezprzewodowych
 - Enumeracja uprawnień
 - Metody enumeracji sekretów i poświadczeń w infrastrukturze oraz aplikacjach
 - Enumeracja udziałów sieciowych
 - Enumeracja WAF (Web Application Firewall)
 - Techniki skanowania z wykorzystaniem decoyów dla zmylenia systemów IDS
 - Ocena podatności systemów ICS
 - Metody automatycznego indeksowania stron i ekstrakcji danych z kodu HTML
- Skanowanie i identyfikacja podatności
 - Techniki wykrywania podatności
 - Narzędzia do wykrywania podatności
 - Typy skanów
 - Skanowanie kontenerów
 - Skanowanie aplikacji
 - Wyszukiwanie haseł i poufnych danych przesyłanych otwartym tekstem
 - Skanowanie sieci
 - Ćwiczenie: skanowanie zidentyfikowanych celów
 - Skanowanie hostów
 - Laboratorium: użycie Metasploit
 - Skanowanie sieci bezprzewodowych
 - Użycie aircrack-ng do wykrywania ukrytych sieci
 - Lokalizacja nieautoryzowanego punktu dostępowego w sieciach bezprzewodowych
 - Walidacja wyników skanów, rozpoznania i enumeracji
 - Laboratorium: rekonesans sieci
 - Skanowanie podatności w systemach Linux
 - Analiza wyników rozpoznania, skanowania i enumeracji

- Kryteria doboru i weryfikacji publicznych exploitów pod kątem bezpieczeństwa
- Walidacja wyników z użyciem skryptów
- Podstawowe koncepcje bezpieczeństwa fizycznego
 - Metody Tailgating jako technika fizycznego uzyskiwania nieuprawnionego dostępu
 - Wizje lokalne
 - Testy z użyciem porzuconych nośników USB jako metoda infekcji systemów
 - Klonowanie identyfikatorów NFC i RFID
 - Otwieranie zamków
 - Dokumentowanie działań związanych ze skanowaniem i identyfikacją podatności
 - Ćwiczenie: identyfikacja koncepcji bezpieczeństwa fizycznego
- Metodyka bezpiecznego przeprowadzania ataków w ramach testów penetracyjnych
 - Przygotowanie i priorytetyzacja ataków
 - Priorytetyzacja celów
 - Identyfikacja zasobów o wysokiej wartości
 - Deskryptory i metryki
 - Oprogramowanie i systemy EOL, EOS
 - Domyślne konfiguracje
 - Uruchomione usługi
 - Słabe metody szyfrowania
 - Dobór technik ataku
 - Dobór i dostosowanie exploitów
 - Procedury dokumentowania ataków
 - Uwzględnianie ograniczeń zakresu testów
 - Ćwiczenie: dostosowanie exploitów
 - Laboratorium: ocena oprogramowania i systemów EOL
 - Laboratorium: wykorzystywanie domyślnych konfiguracji z użyciem Responder
 - Automatyzacja z użyciem skryptów
 - Rodzaje automatyzacji skryptowej
 - PowerShell
 - Bash
 - Python
 - Breach and Attack Simulation (BAS)
 - Laboratorium: uruchamianie skryptów do automatyzacji zadań
- Ataki na aplikacje webowe i w chmurze
 - Ataki webowe
 - Przegląd ataków na aplikacje webowe

- Typy ataków na aplikacje webowe
- Narzędzia do ataków na aplikacje webowe
- Ataki brute force
- Ataki kolizyjne
- Wykrywanie i wykorzystywanie podatności przejścia przez ścieżki w aplikacjach
- Ataki typu request forgery
- Metodyka wykrywania i wykorzystania podatności w procesach deserializacji
- Ataki typu injection
- Ćwiczenie: ataki injection
- Testowanie błędów w logice autoryzacji poprzez modyfikację identyfikatorów obiektów
- Przechwytywanie identyfikatorów sesji w celu uzyskania nieautoryzowanego dostępu
- Ataki typu ACE i techniki zdalnego wykonywania dowolnego kodu w systemie
- Ataki typu File Inclusion i ryzyko zdalnego oraz lokalnego wczytywania zasobów
- Nadużycia API
- Manipulacja JWT
- Laboratorium: ocena bazy danych z użyciem SQLMap
- Laboratorium: wykorzystanie directory traversal do przeprowadzenia ataku
- Laboratorium: wykonywanie XSS
- Laboratorium: nadużycia IDOR
- Laboratorium: poruszanie się lateralne
- Laboratorium: wykorzystanie technik RFI i LFI
- Ataki w chmurze
 - Analiza wektorów ataku na infrastrukturę chmurową oraz usługi SaaS i PaaS
 - Typy ataków w chmurze
 - Narzędzia do ataków w chmurze
 - Ataki na usługę metadanych
 - Błędne konfiguracje zarządzania dostępem
 - Integracje ze stronami z rozwiązaniami stron trzecich
 - Błędne konfiguracje zasobów
 - Ćwiczenie: ataki na błędne konfiguracje zasobów
 - Ujawnianie informacji w logach
 - Modyfikacja obrazów i artefaktów
 - Charakterystyka ataków typu supply chain i ryzyko infekcji łańcucha dostaw
 - Metodyka eksploatacji podatności w procesach automatycznego uruchamiania usług

- Ucieczka malware z konturu
- Nadużycia relacji zaufania
- Wykonanie i analiza ataku typu SYN flood
- Ataki w środowisku enterprise
 - Wykonywanie ataków sieciowych
 - Typy ataków sieciowych
 - Narzędzia do ataków sieciowych
 - Domyślne poświadczenia
 - Atak on-path (MITM)
 - Eksploatacja infrastruktury klucza publicznego (PKI) w celu eskalacji uprawnień
 - Wykorzystywanie domyślnych ustawień oraz luk w uprawnieniach serwisów
 - Techniki VLAN hopping i metody przełamywania izolacji sieci wirtualnych
 - Analiza ryzyka związanego z urządzeniami posiadającymi interfejsy w wielu segmentach sieci
 - Techniki NTLM Relay i metody przejmowania sesji bez łamania haseł
 - Omijanie IDS
 - Laboratorium: praktyczne ćwiczenia z przechwytywania oraz dekodowania ruchu sieciowego
 - Laboratorium: praktyczne zastosowanie silnika skryptowego Nmap w wykrywaniu podatności
 - Laboratorium: praktyczna weryfikacja błędów konfiguracji i banerów usług przez Netcat
 - Laboratorium: symulacja ataku NTLM Relay i przejmowania uprawnień w czasie rzeczywistym
 - Wykonywanie ataków na uwierzytelnianie
 - Typy ataków na uwierzytelnianie
 - Narzędzia do przeprowadzania ataków na uwierzytelnianie
 - MFA fatigue (zmęczenie/presja na potwierdzenia MFA)
 - Ataki pass-the-hash
 - Ataki pass-the-ticket
 - Ataki pass-the-token
 - Ataki na Kerberos
 - LDAP injection
 - Ataki słownikowe
 - Łamanie hasła z użyciem narzędzia John the Ripper
 - Ataki brute force
 - Przeprowadzanie ataków słownikowych na wielu użytkownikach przy użyciu popularnych haseł

- Masowe testowanie przejętych poświadczeń w celu przejęcia kont w innych serwisach
- Ataki na OpenID Connect
- Ataki na SAML
- Laboratorium: łamanie haseł
- Wykonywanie ataków na hosty
 - Typy ataków na hosty
 - Narzędzia do przeprowadzania ataków na hosty
 - Eskalacja uprawnień
 - Zrzuty poświadczeń
 - Omijanie narzędzi bezpieczeństwa
 - Czyszczenie polityk audytu
 - Wykorzystanie błędów konfiguracyjnych
 - Zaciemnianie logiki payloadu
 - Obejście kontroli UAC
 - Ucieczka z powłoki
 - Ucieczka z kiosku
 - Library injection
 - Analiza podatności na wstrzykiwanie bibliotek współdzielonych do zaufanych aplikacji
 - Metody maskowania złośliwej aktywności poprzez nadpisywanie pamięci procesów
 - Usuwanie i modyfikacja wpisów w dziennikach zdarzeń przez napastnika
 - Analiza mechanizmu poszukiwania plików wykonywalnych przez system Windows przy braku cudzysłowów
 - Laboratorium: praktyczna realizacja ataku typu Man-in-the-Middle w celu modyfikacji ruchu
 - Laboratorium: techniki eskalacji uprawnień
 - Laboratorium: praktyczne techniki zaciemniania kodu i modyfikacji sygnatur złośliwego oprogramowania
 - Laboratorium: wykorzystanie metod Blind, Error-based oraz Union-based SQLi
 - Laboratorium: użycie zaufanych narzędzi systemowych do wykonywania złośliwych zadań
 - Laboratorium: wykorzystanie narzędzi do kradzieży skrótów haseł i biletów Kerberos
- Ataki specjalistyczne
 - Ataki na sieci bezprzewodowe
 - Typy ataków bezprzewodowych
 - Narzędzia do przeprowadzania ataków bezprzewodowych

- Aktywność: przegląd narzędzi bezprzewodowych
- Wardriving
- Ataki na Bluetooth
- Atak typu Evil Twin
- Zagłuszanie sygnału w sieciach bezprzewodowych
- Automatyczne testowanie odporności usług poprzez wysyłanie nieoczekiwanych danych
- Metodyka packet craftingu i ręcznego konstruowania nietypowych ramek sieciowych
- Wymuszanie ponownego uwierzytelnienia dla potrzeb krakowania haseł
- Analiza bezpieczeństwa punktów dostępowych z wymuszonym logowaniem przez stronę WWW
- Eksploatacja słabości protokołu WPS i metod siłowego odgadywania kodu PIN
- Ataki socjotechniczne
 - Typy ataków socjotechnicznych
 - Narzędzia do przeprowadzania ataków socjotechnicznych
 - Phishing, whaling, spear phishing i smishing
 - Wykorzystanie socjotechniki do zbierania informacji
 - Watering hole atak
 - Wyłudzenie poświadczeń
 - Laboratorium: ataki socjotechniczne z użyciem SET
- Ataki na systemy specjalistyczne
 - Typy ataków na systemy specjalistyczne
 - Narzędzia do przeprowadzania ataków na systemy specjalistyczne
 - Ataki na urządzenia mobilne
 - Ataki z wykorzystaniem AI
 - Ataki na infrastrukturę OT i ICS
 - Realizacja specjalistycznych ataków w testach penetracyjnych
- Realizacja zadań w testach penetracyjnych
 - Techniki zachowania trwałego dostępu do infrastruktury po restarcie hosta
 - Zasady ustanawiania i utrzymywania trwałego dostępu do systemu
 - Zadania harmonogramów w systemach
 - Tworzenie usług
 - Reverse i bind shells
 - Dodawanie nowych kont
 - Pozyskiwanie prawidłowych poświadczeń kont
 - Klucze rejestru

- Frameworki Command and Control
- Backdoor i Rootkity
- Rozszerzenia przeglądarek i ich wykorzystanie do ataków
- Manipulowanie kontrolami bezpieczeństwa w systemach operacyjnych
- Laboratorium: konfiguracja reverse i bind shells
- Laboratorium: ustanawianie persystencji i inne działania post-exploitation
- Analiza wektorów ataku umożliwiających penetrację kolejnych segmentów infrastruktury
 - Różnice między rozszerzeniem dostępu wewnątrz segmentu a eskalacją przywilejów
 - Skanowanie otwartych portów z komputera zdalnego
 - Metodyka Lateral Movement: od przejścia stacji roboczej do kompromitacji domeny
 - Wykorzystanie zestawów narzędzi takich jak Impacket, Cobalt Strike i BloodHound
 - Tunelowanie ruchu i ustanawianie połączeń typu Proxy w celu penetracji sieci wewnętrznej
 - Implementacja punktów pośredniczących do przekazywania autoryzacji w czasie rzeczywistym
 - Skan z użyciem Zenmap
 - Obejście Windows Firewall
 - Wykorzystanie w atakach WMI i WinRM
- Analiza kanałów eksfiltracji danych i sposobów maskowania transferu informacji
 - Podstawy eksfiltracji danych
 - Pozyskiwanie danych z celu
 - Ukrywanie plików z użyciem OpenStego
 - użycie Alternate Data Streams
 - Laboratorium: techniki eksfiltracji informacji z użyciem alternatywnych strumieni danych w systemie NTFS
- Czyszczenie i przywracanie stanu
 - Procedury czyszczenia i przywracania stanu sprzed ataku
 - Dokumentowanie wykonania zadań w testach penetracyjnych
- Raportowanie i rekomendacje
 - Elementy raportu z testu penetracyjnego
 - Tworzenie raportu z testu penetracyjnego
 - Aspekty raportowania
 - Elementy i definicje w raporcie
 - Specyfikacja dokumentacji i dopasowanie formatu
 - Ocena ryzyka
 - Ograniczenia testu i założenia

- Analiza ustaleń i rekomendacje działań naprawczych
 - Przegląd analizy ustaleń i tworzenia rekomendacji
 - Kontrole techniczne
 - Kontrole administracyjne
 - Kontrole operacyjne
 - Kontrole fizyczne
 - Aktywność: kontrole administracyjne i operacyjne

Wymagania:

Rekomendowane doświadczenie: 3-4 lata pracy na stanowisku pentestera, a także wiedza na poziomie Network+ i Security+ (lub równoważna).

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę CompTIA. Kurs pomaga przygotować się do egzaminu certyfikacyjnego CompTIA PenTest+ (PT0-003), który jest dostępny w centrach egzaminacyjnych Pearson VUE.

Każdy uczestnik autoryzowanego szkolenia CompTIA PenTest+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA PenTest+ (PT0-003).

Prowadzący:

Autoryzowany trener CompTIA