kod szkolenia: PenTest+ / PL DL 5d NIS2

CompTIA PenTest + - szkolenie autoryzowane

Zobacz film: https://youtu.be/AMMd7j0ZMSg

Szkolenie CompTIA PenTest+ (PT0-003) to zaawansowany kurs skierowany do profesjonalistów IT, którzy pragną pogłębić swoje umiejętności w zakresie testów penetracyjnych i oceny podatności systemów. Certyfikat PenTest+ jest uznawany na całym świecie i stanowi doskonałe narzędzie do rozwoju kariery w obszarze cyberbezpieczeństwa.

Dla kogo jest to szkolenie? Szkolenie jest idealne dla osób z doświadczeniem w pracy na stanowiskach takich jak tester penetracyjny, konsultant ds. bezpieczeństwa czy analityk podatności.

Co zyskasz dzięki certyfikacji PenTest+? Po ukończeniu szkolenia i zdaniu egzaminu, otrzymasz certyfikat, który poświadcza Twoje umiejętności w zakresie testowania penetracyjnego i zarządzania podatnościami na poziomie średniozaawansowanym. Zdobędziesz wiedzę i kompetencje niezbędne do przeprowadzania testów penetracyjnych, analizy podatności, opracowywania raportów oraz wdrażania działań naprawczych.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**
- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**
- **ECIH - Certified Incident Handler**
- **Testy penetracyjne (PenTest+, CPENT)**
- **CompTIA SecurityX (Formerly CASP+)**
- **CompTIA SecAI+**
- **CompTIA Linux+**

Odbiorcy szkolenia

Szkolenie skierowane jest do:

- Tester penetracyjny
- Konsultant ds. bezpieczeństwa
- Specjalista ds. bezpieczeństwa w chmurze
- Tester penetracyjny aplikacji webowych
- Specjalista ds. bezpieczeństwa i sieci
- Inżynier bezpieczeństwa informacji
- Analityk podatności

Korzyści

Dlaczego warto wybrać PenTest+?

- **Międzynarodowe uznanie** – Certyfikat PenTest+ to uznawany na całym świecie, neutralny wobec dostawców certyfikat, który stanowi potwierdzenie kompetencji w zakresie testów penetracyjnych i oceny bezpieczeństwa.
- **Przygotowanie do rynkowych wyzwań** – W obliczu rosnącego zagrożenia cyberbezpieczeństwa, organizacje poszukują profesjonalistów zdolnych do przeprowadzania testów penetracyjnych oraz oceny podatności. Certyfikat PenTest+ sprawia, że stajesz się atrakcyjnym kandydatem na rynku pracy.
- **Szersze możliwości kariery** – Certyfikacja otwiera drzwi do ról takich jak tester penetracyjny, konsultant ds. bezpieczeństwa, analityk podatności, specjalista ds. bezpieczeństwa w chmurze czy inżynier bezpieczeństwa informacji.
- **CompTIA PenTest+ –** to jedyny produkt na rynku, który obejmuje zagadnienia związane z sztuczną

inteligencją (AI), praktyczne ćwiczenia z inwentaryzacji, skanowania i analizy, ataków, ruchu – lateral movement, a także planowania, określania zakresu oraz zarządzania podatnościami.

- **Hands-on task –** wymagają od kandydata wykazania kluczowych umiejętności w zakresie testów penetracyjnych dla wszystkich faz ataków, w tym chmury, aplikacji webowych, systemów APIs, Internetu Rzeczy (IoT), środowisk lokalnych (on-premises) oraz hybrydowych sieci.
- **Analiza wyniku** każdej fazy testu penetracyjnego, pozwali: opracować pisemny raport, skutecznie komunikować ustalenia interesariuszom oraz dostarczyć praktyczne rekomendacje.

Program szkolenia

1. Testy penetracyjne – zanim zaczniesz
   - Etyka, aspekty prawne i zgodność z regulacjami
   - Rodzaje dokumentacji i zakres testów
   - Struktura raportu z testu penetracyjnego
   - Rola komunikacji i współpracy w zespole pentesterskim
   - Przegląd popularnych frameworków: PTES, OSSTMM, MITRE ATT&CK, OWASP
   - Automatyzacja i skrypty w testach
2. Zastosowanie działań przed-testowych
   - Definiowanie zakresu: regulacje, cele, obszary, adresy
   - Typy umów: NDA, MSA, SLA, SoW
   - Dobór celów i targetów (web, sieć, mobilne, IoT, API)
   - Modele odpowiedzialności (klient, dostawca, pentester)
   - Planowanie testu, dokumentacja, zasady eskalacji
3. Enumeracja i rozpoznanie
   - Rekonesans: aktywny i pasywny, OSINT, narzędzia (Shodan, theHarvester, Censys)
   - Enumeracja: usług, systemów, DNS, użytkowników
   - Skrypty i automatyzacja rekonesansu (Nmap NSE, PowerShell, Python)
   - Mapowanie ścieżek ataku, BloodHound, SNMP
4. Skanowanie i identyfikacja podatności
   - Techniki wykrywania podatności (DAST, SAST, OpenVAS, Nessus)
   - Skany aplikacji, kontenerów, sieci, hostów, skanowanie tajemnic (TruffleHog)
   - Walidacja wyników i eliminacja false positive
   - Aspekty bezpieczeństwa fizycznego (USB drops, tailgating, lock picking)
5. Przeprowadzanie ataków pentestowych
   - Priorytetyzacja celów: HVA, EOL, słabe konfiguracje
   - Selekcja i dostosowanie exploitów (Metasploit, Responder, CME)
   - Skrypty automatyzujące ataki (Bash, PowerShell, Python)
   - Dokumentacja ścieżek ataku
6. Ataki webowe i w chmurze

- Ataki webowe: SQLi, XSS, RFI/LFI, JWT abuse, IDOR, CSRF, SSRF
- Narzędzia: sqlmap, Burp Suite, ZAP, Postman
- Ataki chmurowe: metadane, IAM, błędne konfiguracje, bucket abuse
- Narzędzia: Pacu, ScoutSuite, Prowler, Kube-hunter

7. Ataki na infrastrukturę korporacyjną
   - Ataki sieciowe: VLAN hopping, IDS evasion, spoofing
   - Ataki uwierzytelniające: MFA fatigue, pass-the-hash, Kerberos
   - Ataki hostowe: privilege escalation, LOLBins, persistence
   - Narzędzia: Metasploit, Hydra, John the Ripper, BloodHound

Self Study :

8. Ataki specjalne
   - Ataki bezprzewodowe: Evil Twin, jamming, fuzzing, WPS PIN
   - Ataki socjotechniczne: phishing, whaling, SET, BeEF
   - Ataki na systemy specjalistyczne: IoT, AI, RFID, OT
9. Zadania poeksploatacyjne i lateral movement
   - Utrzymywanie dostępu: reverse/bind shell, konta, backdoor
   - Mechanizmy C2: Empire, Mythic, Covenant
   - Ruch lateralny i pivoting: WMI, WinRM, LOLBins, sshuttle
   - Ukrywanie aktywności i exfiltracja danych (ADS, OpenStego)
10. Raportowanie i rekomendacje
    - Komponenty raportu: executive summary, findings, narrative, remediation
    - Scoring ryzyka: CVSS, CWE, CVE
    - Dobór kontroli: techniczne, administracyjne, operacyjne, fizyczne
    - Formatowanie i profesjonalna prezentacja wyników

Oczekiwane przygotowanie uczestnika

Szkolenie jest idealne dla osób z doświadczeniem w pracy na stanowiskach takich jak tester penetracyjny, konsultant ds. bezpieczeństwa czy analityk podatności.

Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Autoryzowany podręcznik: The Official CompTIA PenTest+ Student Guide PT0-003

- Środowisko laboratoryjne do pracy własnej – ważne 12 miesięcy

Metoda szkolenia

- wykład
- warsztaty (roczny dostęp do self study)

Czas trwania

5 dni / 35 godzin

Język

Szkolenie: polski
Materialy: angielski