

Wi-Fi Security Testing – Testowanie bezpieczeństwa sieci bezprzewodowych - pentesty

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](#)



Odbiorcy szkolenia

Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji. Osoby nie będące specjalistami z zakresu bezpieczeństwa IT będą mogły zwiększyć świadomość dotyczącą zagrożeń oraz poznać różne metody ataków na sieci bezprzewodowe powszechnie stosowane

przez hakerów.

Również specjaliści ds. bezpieczeństwa informatycznego, audytorzy i tzw. security officers będą mogli ugruntować, usystematyzować bądź uzupełnić swoją wiedzę z zakresu bezpieczeństwa Wi-Fi.



Korzyści

Szkolenie dostarczy uczestnikom wiedzy z zakresu testowania bezpieczeństwa sieci bezprzewodowych. Nauczą się obsługi najczęściej wykorzystywanych narzędzi do testowania bezpieczeństwa Wi-Fi oraz poznają najczęściej stosowane metody ataków na sieci bezprzewodowe. Uczestnicy dokonują kontrolowanych włamań do sieci bezprzewodowej „ofiary” i zdobywają praktyczne umiejętności efektywnej ochrony sieci Wi-Fi.



Program szkolenia

- Protokoły zabezpieczające sieci bezprzewodowe,
- Bezpieczeństwo otwartych sieci bezprzewodowych,
- Sieci gościnne i separacja sieci bezprzewodowych,
- Metody i narzędzia testowania bezpieczeństwa sieci bezprzewodowych,
- Testy bezpieczeństwa sieci bezprzewodowej WEP,
- Testy bezpieczeństwa sieci bezprzewodowej WPA/WPA2,
- Testy bezpieczeństwa sieci ukrytych/bez nazwy,
- Testy bezpieczeństwa sieci z włączonym WPS,
- Odzyskiwanie hasła sieciowego z handshake'u i klucza PMKID,
- Mity dotyczące zabezpieczeń sieci bezprzewodowych,
- Monitorowanie sieci bezprzewodowych,
- Dobre praktyki w bezpieczeństwie sieci bezprzewodowych,
- Bezpieczeństwo IoT w sieciach bezprzewodowych,
- Modyfikowanie urządzenia sieciowe,
- Mikrokontrolery i mikrokomputery w bezpieczeństwie Wi-Fi,
- Modyfikowane urządzenia mobilne,



Oczekiwane przygotowanie uczestnika

Ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.



Szkolenie obejmuje

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty



Czas trwania

2 dni / 14 godzin

Język

- Szkolenie: polski
- Materiały: polski