Tytuł szkolenia: Wprowadzenie do testów penetracyjnych – „etyczny haking” i oceny bezpieczeństwa systemów IT

Kod szkolenia: INFRA-BEZP-PENETR

Wprowadzenie

Szkolenia jest ukierunkowane na zapoznanie się z obecnymi wymaganiami dla organizacji i prowadzenia testów penetracyjnych oraz rozwiązań oceny bezpieczeństwa. Podczas szkolenia zapoznasz się jak przygotować się do testów penetracyjnych, jakie są poszczególne etapy testu w środowisku IT. W oparciu o jakie oprogramowanie, standardy i wytyczne przeprowadzić testy oraz ocenę bezpieczeństwa a także jak przygotować raport końcowy.

Adresaci szkolenia

Szkolenie adresowane jest do osób które będą odpowiedzialne za bezpieczeństwo systemów IT w organizacji, audytorów wewnętrznych, administratorów bezpieczeństwa informacji a także do osób na co dzień zajmujących się problematyką bezpieczeństwa i zarządzania bezpieczeństwem systemów teleinformatycznych, odpowiedzialnych za bezpieczeństwo i kontrolę stanu bezpieczeństwa w systemach teleinformatycznych.

Cel szkolenia

Celem szkolenia jest przedstawienie zakresu wiedzy na temat organizacji testów penetracyjnych, poszczególnych etapów od przygotowania po realizację testów wraz z działaniami i ustaleniami, które należy ująć w raporcie końcowym z rekomendacjami. Ponadto w ramach szkolenia zaprezentowane zostaną aplikacje i metodologie prowadzenia testów penetracyjnych oraz oceny bezpieczeństwa systemów IT.

Czas i forma szkolenia

- 14 godzin (2 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Wprowadzenie do testów penetracyjny i oceny bezpieczeństwa
2. Aspekty prawne oraz wymagania organizacyjne
3. Metodyki testów penetracyjnych oraz rekomendacje
    a. OWASP, NIST , OSSTMM,
4. Elementy testów penetracyjnych
    a. Rekonesans,
    b. Enumeracj
    c. Mapowanie,
    d. Socjotechnika,
    e. „Atak”,
    f. Podnoszenie uprawnień,
    g. Utrzymanie dostępu.
5. Aplikacje wspierające działania „etycznego hakera”
6. Raport wraz z ustaleniami z przeprowadzonych działań