Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Etyczny Hacking i Testy Penetracyjne w Kali Linux

Opis

Intensywne, 3-dniowy warsztat z etycznego hackingu w Kali Linux pozwoli na zdobycie praktycznych umiejętności niezbędne w branży cybersecurity. Opanujesz narzędzia takie jak Nmap i Burp Suite oraz nauczysz się przeprowadzać kontrolowane ataki SQL Injection, XSS czy IDOR.

Zdobądź twarde kompetencje pentestera pod okiem doświadczonego praktyka w celu profesjonalnego zabezpieczaniu aplikacji webowych oraz infrastruktury sieciowej.

Umiejętności

Dzięki szkoleniu;

konfigurujesz profesjonalne środowisko testowe oparte na systemie Kali Linux w środowisku wirtualnym VirtualBox.

przeprowadzisz kompleksowy rekonesans (OSINT) oraz zidentyfikujesz potencjalne wektory wejścia do badanej domeny.

nauczysz się wykrywać ukryte hosty, otwarte porty oraz aktywne usługi sieciowe przy użyciu zaawansowanych technik skanowania w Nmap.

opanujesz obsługę Burp Suite – kluczowego narzędzia do przechwytywania i modyfikowania ruchu HTTP/HTTPS.

przełamiesz zabezpieczenia aplikacji webowych, wykonując kontrolowane ataki SQL Injection, Cross-Site Scripting (XSS) oraz IDOR.

wykorzystasz publiczne bazy podatności (Exploit-DB) do wyszukiwania i dopasowywania gotowych exploitów

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Dla kogo?

Szkolenie przeznaczone jest dla administratorów sieci i systemów, młodszych specjalistów ds. bezpieczeństwa (Junior Pentesterów), programistów (Dev/DevSecOps) oraz pracowników wsparcia IT posiadających podstawową znajomość środowiska Linux

Szczegółowy program szkolenia

1. Instalacja i konfiguracja Kali Linux na Virtual Box
2. Podstawowe polecenia, zbieranie informacji o systemie, procesy, usługi
    a. Wyszukiwanie
    b. Operacje na plikach
    c. Zarządzanie użytkownikami i uprawnieniami
3. Rekonesans – odkrywanie domen, subdomen
    a. Wprowadzenie do OSINT
    b. Sprawdzanie domen pod kątem możliwych dróg wejścia do systemu
4. Skanowanie portów, enumeracja usług, praca z nmap
    a. Skanowanie sieci
    b. Odkrywanie hostów
5. Identyfikowanie podatności
6. Wprowadzenie do programu Burp Suite
    a. Instalacja i konfiguracja
    b. Podstawowe funkcjonalności przydatne w etycznym hackingu
7. Eksploitacja systemów, aplikacji i usług
    a. Ręczna eksploitacja
    b. Wykorzystanie baz danych eksploitów (https://www.exploit-db.com/)
8. Atakowanie aplikacji webowych
    a. Podatności IDOR
    b. Ataki na formularze
    c. SQL Injection
    d. XSS

Liczba dni, liczba godzin szkoleniowych

3 dni, 24 godziny szkoleniowe

Ścieżka rozwoju po szkoleniu

- *AI w cyberbezpieczeństwie*