Szkolenie CEH v 13- Certified Ethical Hacker AI

Szkolenie akredytowane przez EC-Council, prowadzone przez akredytowanego trenera z użyciem akredytowanych materiałów i środowiska szkoleniowego (ilabs/CQ Labs), dostarczanego przez ECC.

Szkolenie musi obejmować min. następujące tematy:

Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)
Zbieranie informacji o ataku (Footprinting and Reconnaissance)
Skanowanie sieci (Scanning Networks)
Enumeracja (Enumeration)
Analiza podatności (Vulnerability Analysis)
Hackowanie systemu (System Hacking)
Złośliwe oprogramowanie (Malware Threats)
Monitorowanie i przechwytywanie danych (Sniffing)
Inżynieria społeczna – socjotechniki (Social Engineering)
Ataki DDoS (Denial-of-Service)
Przejęcie/przechwytywanie sesji (Session Hijacking)
Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)
Hakowanie serwerów sieciowych (Hacking Web Servers)
Hakowanie aplikacji internetowych (Hacking Web Applications)
Ataki przez zapytania w SQL (SQL Injection)
Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)
Hakowanie mobilnych platform (Hacking Mobile Platforms)
Hakowanie Internetu Rzeczy (IoT  Hacking)
Bezpieczeństwo chmury (Cloud Computing)
Kryptografia (Cryptography)

Szkolenie dla 3 osób, czas trwania szkolenia min 5 dni (40 godzin). Szkolenie zakończone certyfikatem uczestnictwa. Szkolenie musi umożliwiać przygotowanie uczestników do zdania egzaminu i tym samym uzyskania certyfikatu Certified Ethical Hacker. Voucher na egzamin z okresem ważności 1 roku musi być zawarty w cenie szkolenia.