**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:

1. Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)
2. Zbieranie informacji o ataku (Footprinting and Reconnaissance)
3. Skanowanie sieci (Scanning Networks)
4. Enumeracja (Enumeration)
5. Analiza podatności (Vulnerability Analysis)
6. Hackowanie systemu (System Hacking)
7. Złośliwe oprogramowanie (Malware Threats)
8. Monitorowanie i przechwytywanie danych (Sniffing)
9. Inżynieria społeczna – socjotechniki (Social Engineering)
10. Ataki DDoS (Denial-of-Service)
11. Przejęcie/przechwytywanie sesji (Session Hijacking)
12. Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)
13. Hakowanie serwerów sieciowych (Hacking Web Servers)
14. Hakowanie aplikacji internetowych (Hacking Web Applications)
15. Ataki przez zapytania w SQL (SQL Injection)
16. Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)
17. Hakowanie mobilnych platform (Hacking Mobile Platforms)
18. Hakowanie Internetu Rzeczy (IoT  Hacking)
19. Bezpieczeństwo chmury (Cloud Computing)
20. 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.