**ZAŁ. NR 6**

**OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI II**

**Szkolenie:**

**Certified Ethical Hacker wraz z certyfikacją**

**Forma szkolenia:** Szkolenie stacjonarne

**Liczba szkolonych osób:** 1

**Minimalne wymagania:** Szkolenie w wymiarze 40 godzin (5 dni) w języku polskim

**Szkolenie ma uwzględniać co najmniej 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)

**Po szkoleniu kursant otrzymuje:**

1. Certyfikat ukończenia szkolenia oraz voucher na egzamin ważny min. 1 rok
2. Dostęp do wirtualnych labów pozwalających na poznanie praktycznej strony hackingu   
   min. na 6 miesięcy
3. Materiały szkoleniowe