



I. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest wybór Wykonawcy usługi **szkolenia z zakresu bezpieczeństwa sieci komputerowych** dla uczestniczek/uczestników projektu realizowanego przez Akademię Humanitas.
2. Celem szkolenia jest podniesienie kompetencji i umiejętności uczestników w zakresie bezpieczeństwa sieci.
3. Szkolenie musi być realizowane w oparciu o laboratoria odwzorowujące rzeczywiste środowisko IT realizujące usługi sieciowe. Każdy uczestnik ma do dyspozycji stanowisko z przygotowanym laboratorium.
4. W trakcie zajęć musi zostać przeprowadzona minimum analiza środowiska sieciowego i usług.
5. Każdy uczestnik musi mieć możliwość zaplanowania, wykonania, a następnie udokumentowania przeprowadzonego przez siebie testu penetracyjnego, na podstawie którego zostanie stworzony raport z przeprowadzonych testów, a także zostaną wdrożone zabezpieczenia eliminujące podatności i luki w usługach.
6. Uczestnikami szkolenia będą osoby uczące (nauczyciele) w Technikum Mechaniczno-Elektrycznym im. Nikoli Tesli w Chorzowie biorące udział w projekcie.
7. Realizacja szkolenia: stacjonarnie lub/i zdalnie.
8. Miejsce realizacji usługi: Przedmiot zamówienia (w przypadku realizacji w formie stacjonarnej) ze względu na grupę docelową, do której kierowane jest wsparcie, realizowany będzie w promieniu maksymalnie 30 km od Technikum Mechaniczno - Elektrycznego im. Nikoli Tesli w Chorzowie liczonej po drogach publicznych w oparciu o <https://www.google.pl/maps> według najszybszej trasy.
9. Czas trwania kursu: minimum 24 godziny dydaktyczne.
10. Liczba osób: 2 osoby. Zamawiający dopuszcza możliwość realizacji usługi poprzez zapewnienie miejsc szkoleniowych w tzw. szkoleniach otwartych.
11. Dni realizacji szkolenia: według ustalonego z Zamawiającym harmonogramu. Możliwe dni realizacji: od poniedziałku do piątku.
12. Wykonawca zapewni materiały szkoleniowe dla każdego uczestnika szkolenia.
13. Uczestnik po szkoleniu otrzyma certyfikat ukończenia szkolenia.
14. Minimalny zakres szkolenia:
 - a. Najważniejsze definicje i odpowiedzialność prawna,
 - b. Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?
 - c. Omówienie faz testu penetracyjnego,
 - d. Planowanie,
 - e. Rekonesans,
 - f. Skanowanie,
 - g. Wtargnięcie, Utrzymanie dostępu
 - h. Zatarcie śladów,



- i. Pasywne i aktywne sposoby zbierania informacji,
- j. Omówienie dostępnych rodzajów ataków,
- k. Łamanie haseł,
- l. Ataki na sieci,
- m. Utrzymanie dostępu,
- n. Backdoor i rootkit,
- o. Zacieranie śladów,
- p. Jak prawidłowo raportować,
- q. Omijanie systemów IDS oraz Firewall,
- r. Fuzzing,
- s. Programy wykorzystywane przez atakujących,
- t. Sposoby ochrony systemów,
- u. Rekonesans podmiotów,
- v. Skanowanie sieci, serwerów oraz usług,
- w. Penetracja sieci,
- x. Ataki phishingowe,
- y. Metody ochrony przed atakami: idea honeypotów, systemy IDS/IPS, metody hardeningu systemów operacyjnych.