Zakres merytoryczny kursu:

- Wprowadzenie do „Etycznego Hakingu".
- Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku.
- Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci.
- Enumeracja – aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze.
- Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru.
- Włamywanie się do systemów („Hakowanie” systemów).
- Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania.
- Podsłuchiwanie (Sniffing) sieci – przechwytywanie danych
- Socjotechniki (Inżynieria społeczna).
- Ataki na odmowę dostępu do usługi (Denial-of-Service).
- Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym.
- Omijanie systemów IDS, firewall’i, honeypot’ów.
- Atakowanie serwerów webowych.
- Atakowanie aplikacji webowych.
- SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL.
- Włamywanie się do sieci bezprzewodowych.
- Hakowanie platform i urządzeń mobilnych.
- Hakowanie "Internetu Rzeczy" oraz "Technologii Operacyjnych" (IoT i OT).
- Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing).
- Kryptografia.