

SZKOLENIE

Zaawansowane metody pozyskiwania informacji z ogólnodostępnych źródeł (OSINT)

Grupa docelowa

Agencje: HR, marketingowe | Detektywi
Dziennikarze | Windykatorzy

Poziom zaawansowania



TRENER

Artur Czyż



- Rocznie realizuje ponad 100 projektów związanych z bezpieczeństwem IT (audyty, testy penetracyjne, szkolenia)
- Aktywnie uczestniczy w programach typu bug bounty, przykłady zgłoszonych błędów: IBM InfoSphere (CVE-2016-0250 / CVE-2016-0280) oraz Swagger UI (CVE-2016-7559 i CVE-2016-7918)
- Prelegent na: Sekurak Hacking Party (2018) oraz Advanced Threat Summit (2014)
- Autor tekstów w serwisie [sekurak.pl](#) oraz w magazynie „Programista”
- Posiada certyfikat Offensive Security Certified Professional
- Konsultant d/s bezpieczeństwa IT w firmie Securitum

PUBLIKACJE

- > [Odczytywanie danych zapisanych na zbliżeniowych kartach płatniczych](#)
- > [Automatyczna analiza złośliwego oprogramowania z wykorzystaniem SysAnalyzer](#)
- > [Nietypowe metody wykorzystywane w atakach phishingowych](#)

ZAPISZ SIĘ

OSZKOLENIU

- ✓ skutecznie uczy, jak znaleźć informacje o konkretnej osobie bądź firmie, bazując na narzędziach, metodach oraz źródłach pozyskiwania danych z wielu nietypowych i nieoczywistych miejsc
- ✓ atrakcyjnie pokazuje, jak łączyć znalezione informacje w celu zobaczenia szerszego kontekstu
- ✓ omawia techniki związane ze zbieraniem informacji, a także uczy rozpoznawać techniki dezinformacji
- ✓ zapoznaje uczestników ze sposobami anonimizacji własnych działań, a także omawia profesjonalne procedury i modele wykorzystywane m.in. przez organy ścigania

UCZESTNICY O TRENERZE

- “Bardzo dobrze przygotowany pod kątem merytorycznym, ogromna wiedza oraz bardzo dobry sposób przedstawienia tematu.
- “Starał się wykorzystać cały dostępny czas. Tematyka była ciekawa i równie ciekawie zaprezentowana.
- “Konkretnie przedstawione i poparte przykładami.
- “Bardzo fajnie prowadzone szkolenie. Jasne i klarowne.
- “Zainteresował audytorium, odpowiadał na pytania.
- “Merytoryczny, dobrze tłumaczył omawiane zagadnienia.

RAMOWY PROGRAM SZKOLENIA

Wprowadzenie

- Czym jest OSINT?
- Typy gromadzenia danych wywiadowczych
- Model SARA (Scanning, Analysis, Response, Assessment)
- Cykl wywiadowczy w kontekście profesjonalnego podejścia do OSINT

Narzędzia i metody pozyskiwania informacji

- Źródła o ograniczonym dostępie:
 - udostępnianie danych z rejestru PESEL
 - udostępnianie danych z Rejestru Dowodów Osobistych
 - Krajowy Rejestr Karny
- Popularne zbiory zasobów, m.in.
 - wyszukiwanie na podstawie nazwy, imienia i nazwiska, adresu e-mail, lokalizacji, zainteresowań, branży, znajomych i wielu innych elementów
 - wyszukiwanie dokumentów i plików tekstowych
 - gazety, czasopisma, radio i telewizja
 - Wikileaks
 - księgi wieczyste
- Dane firmowe
 - strategie zbierania danych (m.in. wartościowe informacje na temat numerów identyfikacyjnych)
 - przegląd centralnych ewidencji i rejestrów (oficjalnych i nieoficjalnych)
- Media społecznościowe (m.in. Facebook, Twitter i inne)
 - przegląd wewnętrznych narzędzi
 - usługi mobilne i stacjonarne
 - zaawansowane konstruowanie zapytań w wyszukiwarce
 - podstawowe informacje o numerach telefonu
 - spis abonentów sieci telefonicznych
 - internetowe bazy numerów telefonów
 - strategie wyszukiwania i zbierania informacji
- Fotografie, obrazy, zdjęcia i wideo
 - analiza fotografii (m.in. tworzenie nawyków prawidłowej obserwacji)

- wyszukiwanie podobnych zdjęć lub ich części (Reverse Image)
- identyfikacja modyfikacji w zdjęciu
- odwracanie efektu „rozmycia” oraz naprawianie uszkodzonych plików
- wydobywanie wartościowych informacji, m.in. współrzędnych GPS
- Systemy informacji geograficznej
 - profesjonalna analiza lokalizacji
 - analiza zdjęć satelitarnych
- Dane o pojazdach (m.in. lądowych, wodnych oraz statkach powietrznych)
 - przegląd oficjalnych i nieoficjalnych rejestrów
 - lokalizowanie pojazdów (części z nich)
- Szczegółowe zbiory danych
 - polityka, turystyka, zdrowie, inne
- Pozyskiwanie informacji technicznych
 - analiza adresu IP
 - analiza domeny (m.in. wyszukiwanie informacji o jej właścicielu)
 - podgląd archiwalnych lub usuniętych danych i informacji na stronach WWW
 - zaawansowane metody wyszukiwania danych w wyszukiwarkach internetowych
 - monitorowanie nowych wyników w wyszukiwarce
- Kryptowaluty
 - wprowadzenie do świata cyfrowych walut
 - podstawy analizy transakcji
- Dark Web
 - przegląd polskich serwisów
 - przegląd zagranicznych serwisów
 - TOR (m.in. wyszukiwarki oraz portale)

Podsumowanie

SZKOLENIE POLECAJĄ