

Informatyka Śledcza - Skuteczne Wykorzystanie Najnowszych Technik IŚ

Szkolenie organizowane jest przez Akademię Linux Magazine, organizatora cyklu warsztatów i szkoleń poświęconych najnowszej wiedzy związanej z zagrożeniami i bezpieczeństwem systemów IT oraz tworzeniem i administrowaniem sieciami i serwerami komputerowymi.

Proponowane przez Akademię przedsięwzięcia kierowane są głównie do sektorów, w których poufność danych posiada najwyższy priorytet. W dzisiejszym świecie jest to kwestia bardzo istotna. Od świadomości zagrożeń i umiejętności ich niwelowania, zarówno w pracy prywatnych firm jak i instytucji użytku publicznego, zależy bezpieczeństwo każdego z nas.

Zasady uczestnictwa: Szkolenie to jest organizowane zarówno jako szkolenie otwarte jak i zamknięte. Koszt szkolenia podany w załączonym na ostatniej stronie formularzu dotyczy szkolenia otwartego. W przypadku szkoleń zamkniętych koszt ustalany jest indywidualnie z zamawiającym. Minimalna liczba uczestników szkolenia to 5 osób, maksymalna 12.

Szkolenie zamknięte może odbyć się we współpracującym z nami ośrodku szkoleniowym lub w siedzibie firmy klienta. Dodatkowo zależnie od potrzeb, program danego szkolenia może zostać dostosowany do wymagań zamawiającego.

Podstawowe informacje o szkoleniu:

*Informatyka śledcza to poszukiwanie i analiza informacji w formie cyfrowej, mająca na celu dostarczenie elektronicznych środków dowodowych popełnionych przestępstw lub nadużyć.**

Handel narkotykami, bronią, środkami zakazanymi, pranie brudnych pieniędzy, oszustwa finansowe, handlowe, gospodarcze, phishing, pharming, carding, hacking, kradzież oprogramowania, własności intelektualnej, danych i informacji, podszywanie się, wymuszenia, wyłudzenia, cyberterrorizm, terrorizm – to zagrożenia, z którymi coraz częściej stykamy się w życiu, a osoby je popełniające coraz częściej i coraz bardziej świadomie wykorzystują technologie IT.

Przestępcy wykorzystujący zdobycze współczesnego świata jako narzędzia w swoim kryminalistycznym procederze, czują się bezkarni. Sądzą, iż ich umiejętności i wiedza pozwalają na ukrycie swoich czynów i własnej osoby w sieci w taki sposób, iż nikt nie jest w stanie trafić na ich trop, nie mówiąc o ukaraniu. Metody i narzędzia informatyki śledczej dostarczają nam niezbędnych środków technicznych, zwiększających szanse ujęcia takich osobników.

* Encyklopedia Internetowa Wikipedia, Informatyka Śledcza, http://pl.wikipedia.org/wiki/Informatyka_%C5%9Bledcza

Zagadnienia poruszone podczas szkolenia:

- Dowody cyfrowe, klasyfikacja i ich problematyka.
- Analizy systemowe.
- Dokumenty informatyki śledczej
- Elementy steganografii, kryptografii, crackingu
- Elementy funkcjonowania systemów operacyjnych.
- Badanie dysków twardych, napędów optycznych, dysków wymiennych, pamięci masowych.
- Odtwarzanie danych, kasowanie danych.
- Zagadnienia IŚ w systemach Unix.
- Analizy chronionych archiwów.
- Identyfikacja danych oraz Analiza rejestrów systemowych.
- Zagadnienia sieciowe P2P. Konwertowanie danych.

Szkolenie skierowane jest do: Funkcjonariuszy Policji, pracowników Prokuratury, pracowników i współpracowników Sądów, Detektywów oraz Agencji Detektywistycznych, pracowników Służb i Jednostek Specjalnych, pracowników oraz funkcjonariuszy Żandarmerii Wojskowej, pracowników Wojska, Straży Granicznej oraz pracowników firm i tych instytucji, które potrzebują poznać podstawy prowadzenia analizy informatycznej w dziedzinie informatyki śledczej.

Najważniejsze korzyści dla uczestników, biorących udział w szkoleniu:

- Poznanie specyficznych metod analizy informatycznej.
- Poznanie technik i narzędzi służących do ukrywania śladów w systemach komputerowych.
- Nabycie umiejętności samodzielnego odszukiwania śladów i dowodów.
- Poszerzenie wiedzy dotyczącej sposobów funkcjonowania systemów operacyjnych i systemów komputerowych.
- Poznanie niezbędnych narzędzi i technik, umożliwiających skuteczne analizy informatyczne.
- Poznanie podstawowych metod zabezpieczania dowodów elektronicznych.

Wymagania względem uczestników: podstawowa znajomość budowy systemów operacyjnych, znajomość systemów plików, tworzenia katalogów oraz plików z poziomu systemu operacyjnego, znajomość protokołów sieciowych. Przydatna będzie także wiedza z zakresu zagadnień data recovery, budowy jednostek PC oraz zasad działania oprogramowania malware.

Informatyka Śledcza - Skuteczne Wykorzystanie Najnowszych Technik IŚ

Agenda - dzień pierwszy

08:20-09:50	<i>Rejestracja</i>
09:50-10:00	<i>Powitanie</i>
10:00-10:40	Wykład: Historia Informatyki Śledczej, Pojęcie Dowodu elektronicznego. Omówione zostaną pojęcia związane z zagadnieniami informatyki śledczej. Przedstawione zostaną dane dotyczące potencjalnych dowodów elektronicznych w systemach komputerowych oraz metody ich klasyfikacji i gromadzenia.
10:40-11:00	<i>Przerwa</i>
11:00-12:20	Wykład: Klasyfikacje i Rekonstrukcje, Odnoszenia czasowe. Analiza behawioralna. Zostaną poruszone tematy dotyczące klasyfikacji i rekonstrukcji zdarzeń oraz metody określania czasów życia informacji i danych. Przedstawimy również sposoby analiz zewidencjonowanych dowodów oraz techniki odtwarzania historii zajścia na podstawie w/w analiz.
12:20-12:40	<i>Przerwa</i>
12:40-13:40	Wykład: Elementy dokumentacji IŚ. Protokoły dokumentacyjne, wzory i wykorzystania. Omówimy cechy funkcjonalne podstawowych dokumentów wykorzystywanych podczas prowadzenia badań systemów komputerowych. Na zajęciach zostaną omówione wzory dokumentów, ich zastosowania i wykorzystania, potrzeby tworzenia oraz inne zagadnienia z nimi związane.
13:40-14:20	<i>Obiad</i>
14:20-17:00	Wykład/Ćwiczenia: Techniki ewidencjonowania i przetwarzania sprzętu IT w zagadnieniach IŚ. Obsługa systemu poddawanego analizie Omówione zostaną tematy związane z uzyskiwaniem dostępu do nośników, sprzętu, systemów oraz innych zasobów poddawanych analizie. Przedstawione będą najlepsze praktyki zachowania w stosunku do wrażliwych danych oraz potencjalnych systemów dowodowych.
17:00-17:10	<i>Podsumowanie I dnia</i>

Agenda - dzień drugi

09:25-09:30	<i>Rozpoczęcie drugiego dnia</i>
09:30-10:30	Wykład: Elementy kryptografii, techniki dostępowe do archiwów i zasobów chronionych Przedstawione zostaną najczęściej wykorzystywane metody szyfrowania danych na dyskach. Uczestnicy dokonają prób złamania tych zabezpieczeń w celu uzyskania dostępu do chronionych informacji. Zostaną również omówione sposoby przełamywania haseł dostępu do kont użytkowników i systemów, a także najskuteczniejsze narzędzia wspierające ten proces.
10:30-10:50	<i>Przerwa</i>
10:50-12:20	Ćwiczenia: Analiza Zasobów chronionych, sposoby uzyskiwania dostępu. Hasła systemów Unix oraz Windows – W trakcie tych zajęć uczestnicy przeprowadzać będą analizy zasobów systemowych, chronionych hasłami.
12:20-12:40	<i>Przerwa</i>
12:40-13:40	Wykład/Ćwiczenia: Formaty plików, możliwość wykorzystania i przetwarzania. Zajęcia te mają na celu demonstrację możliwości niezgodnego z normami i wytycznymi, posługiwania się plikami. Zostaną zaprezentowane metody ukrywania danych, w tym kodów wykonywalnych.
13:40-14:20	<i>Obiad</i>
14:20-16:30	Wykład/Ćwiczenia: Narzędzia informatyki śledczej. Głównym celem tego spotkania jest zaznajomienie się i praktyczne poznanie najczęściej wykorzystywanych narzędzi w informatyce śledczej.
16:30-16:30	<i>Podsumowanie II dnia</i>

Agenda - dzień trzeci

09:25-09:30	<i>Rozpoczęcie trzeciego dnia</i>
09:30-10:30	Ćwiczenia: Sygnatury plików, Rejestry, Pliki Dzienników. Zajęcia te mają na celu zaznajomienie z aspektami analizy rejestrów, plików dziennika oraz innych typowych elementów systemowych dla platform Unix oraz Windows.
10:30-10:50	<i>Przerwa</i>
10:50-13:00	Ćwiczenia: Elementy Data Recovery. Podczas tych zajęć, uczestnicy zostaną zaznajomieni z sposobami odzyskiwania danych z nośników takich jak dyski twarde, dyski przenośne, karty sd oraz inne. Zostaną omówione sposoby wyszukiwania usuniętych danych oraz narzędzia to automatyzujące.
13:00-13:20	<i>Przerwa</i>
13:20-14:50	Ćwiczenia: Analiza przypadku – kompleksowa analiza danych. Podsumowaniem spotkań będzie praktyczna analiza całego systemu. Zakresem ostatnie zajęcia będą obejmować praktyczne i teoretycznie umiejętności nabyte w trakcie całego szkolenia.
14:50-15:00	<i>Podsumowanie i zakończenie</i>
15:00-15:40	<i>Obiad</i>