

Szkolenie: The Linux Foundation  
LFS416 Linux Security

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	5800 PLN NETTO*	4 dni
Stacjonarne	Tablet CTAB	6200 PLN NETTO*	4 dni
Metoda dlearning	Tradycyjne	5800 PLN NETTO*	4 dni
Metoda dlearning	Tablet CTAB	5800 PLN NETTO*	4 dni

\* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

## LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

## DOSTĘPNE TERMINY

2019-10-08 | 4 dni | Warszawa (Promocja)

2019-10-08 | 4 dni | Warszawa

2019-11-26 | 4 dni | Kraków (Promocja)

2019-11-26 | 4 dni | Kraków

## Cel szkolenia:

Ten zaawansowany, całkowicie praktyczny kurs w sposób techniczny zapoznaje uczestników z ważnymi narzędziami i technikami bezpieczeństwa. Zwracając uwagę zarówno na środki ataku i możliwe luki bezpieczeństwa; kurs zapewnia kompletny poradnik jak osłabiać ryzyko ataku w dowolnym środowisku Linux.

Podczas kursu **LFS416 Linux Security** nauczysz się:

- Jak oszacować zagrożenie bezpieczeństwa w środowisku Linuksa
- Najlepszych technik i narzędzi do zwiększania bezpieczeństwa
- Uodporniania serwera
- Jak wdrażać i używać narzędzi do monitorowania i wykrywania ataków
- Jak dostrzec możliwe podatności
- Sztuki projektowania polityki bezpieczeństwa Linuksa i strategii reagowania
- Jak skonfigurować system w zgodności z HIPAA, DISA STIG itp.

Ten kurs jest przeznaczony do pracy z szeroką gamą dystrybucji Linuksa, więc będziesz mógł zastosować te koncepcje niezależnie od swojej dystrybucji.

## Plan szkolenia:

- Wprowadzenie
  - Linux Foundation
  - Linux Foundation Training
  - Linux Foundation Certifications
  - Laboratory Exercises, Solutions and Resources
  - E-Learning Course: LFS216
  - Szczegóły dystrybucji
  - Laboratoria
- Podstawy bezpieczeństwa
  - Czym jest bezpieczeństwo?
  - Szacowanie
  - Zapobieganie
  - Wykrywanie
  - Reagowanie
  - Laboratoria
- Szacowanie ryzyka i zagrożenia
  - Klasy ataków
  - Rodzaje ataków
  - Kompromisy
  - Laboratoria
- Dostęp fizyczny
  - Fizyczne bezpieczeństwo
  - Bezpieczeństwo sprzętu
  - Zrozumienie procesu rozruchu Linuksa
  - Laboratoria
- Prowadzenie logów
  - Przegląd logów
  - Usługi Syslog
  - Audit Daemon jądra Linuksa
  - Logi zapory sieciowej
  - Raporty logów
  - Laboratoria
- Audytywanie i wykrywanie
  - Podstawy audytowania

- Zrozumienie rozwoju ataku
- Wykrywanie ataku
- Systemy wykrywania włamań
- Laboratoria
- Bezpieczeństwo aplikacji
  - Błędy i narzędzia
  - Śledzenie i dokumentowanie zmian
  - Kontrola dostępu do zasobów
  - Techniki łagodzenia
  - Frameworki kontroli dostępu oparte na polityce
  - Rzeczywisty przykład
  - Laboratoria
- Podatności jądra
  - Przestrzeń użytkownika i jądra
  - Błędy
  - Zmniejszanie podatności jądra
  - Przykłady podatności
  - Laboratoria
- Uwierzytelnianie
  - Szyfrowanie i uwierzytelnianie
  - Hasła i PAM
  - Sprzętowe tokeny
  - Uwierzytelnianie biometryczne
  - Sieć i scentralizowane uwierzytelnianie
  - Laboratoria
- Lokalne bezpieczeństwo systemu
  - Standardowe uprawnienia UNIX
  - Konto administratora
  - Zaawansowane uprawnienia UNIX
  - Spójność systemu plików
  - Kwoty dyskowe
  - Laboratoria
- Bezpieczeństwo sieci
  - Przegląd protokołów TCP/IP
  - Zdalne Trust Vectors
  - Zdalne Exploity

- Laboratoria
- Bezpieczeństwo usług sieciowych
  - Narzędzia sieciowe
  - Bazy danych
  - Serwery www
  - Serwery plików
  - Laboratoria
- Denial of Service
  - Podstawy sieci
  - Metody DoS
  - Techniki minimalizacji
  - Laboratoria
- Zdalny dostęp
  - Niezaszyfrowane hasła
  - Uzyskiwanie dostępu do systemów Windows
  - SSH
  - IPSEC VPN
  - Laboratoria
- Zapory sieciowe i filtrowanie pakietów
  - Podstawy zapór sieciowych
  - iptables
  - Implementacja Netfilter
  - Zarządzanie regułami Netfilter
  - Minimalizacja prób logowania typu brute force
  - Laboratoria
- Reagowanie i łagodzenie
  - Przygotowanie
  - W trakcie zdarzenia
  - Radzenie sobie z następstwami zdarzenia
  - Laboratoria
- Testowanie zgodności z OSCP
  - Testowanie zgodności
  - Wprowadzenie do SCAP
  - OpenSCAP
  - SCAP Workbench
  - Skanowanie w wierszu poleceń

- Laboratoria

## Wymagania:

Uczestnicy powinni:

- Wykazywać się silnym zrozumieniem podstawowych założeń sieci i administracji lokalnymi systemami (wiedza odpowiadająca zakresowi kursów **LFS301 Linux System Administration** oraz **LFS311 Linux Networking i Administration**)
- Posiadać doświadczenie z Linuksem (lub, bardziej ogólnie, UNIX'em), zwłaszcza na poziomie wiersza poleceń.

## Poziom trudności



## Certyfikaty:

Uczestnicy otrzymają **certyfikat** podpisany przez **The Linux Foundation**.

## Prowadzący:

Certyfikowany trener The Linux Foundation.