Training: OffSec
OffSec Security Fundamentals

OffSec | Learning Partner

TRAINING GOALS:

Security Fundamentals from OffSec, delivered over 5 days with an OffSec authorized trainer. OffSec Security Fundamentals cover the following modules:

- PEN-100 Network Penetration Testing Essentials
- WEB-100 Web Application Assessment Essentials
- EXP-100 Exploit Development Essentials
- SOC-100 Security Operations Essentials
- CLD-100 Introduction to Cloud Security
- SSD-100 Introduction to Secure Software Development

OffSec Security Fundamentals (OffSec 100-level) content is designed to help learners adopt basic cybersecurity-adjacent concepts, cultivate the mindset necessary for a successful cybersecurity career, and provide the prerequisites for OffSec's advanced courses, including the PEN-200 (OSCP) and SOC-200 (OSDA).

Beside of 5 days ILT/VILT with an OffSec authorized instructor you will also gain:

- 1 year of unlimited access to all OffSec fundamental content
- 365 days of lab access
- PEN-103 Kali Linux Reinvented + 1 KLCP exam attempt
- PEN-210 Foundational Wireless Network Attacks + 1 OSWP exam attempt

Benefits

By completing the PEN-100, WEB-100, EXP-100, SOC-100, CLD-100, SSD-100 modules, learners will:

- Obtain basic IT and information security skills, get equipped with introductory cyber defense knowledge, elevate their skill set in web application security, et introduced to the essentials of exploit development, boost their fundamental knowledge of cloud security, become immersed in secure software development

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Get prepared to advance their skills and enroll in PEN-200, SOC-200, WEB-200
- Start their preparation for entry-level security roles
- Test their progress and the level of preparedness with Assessments and Badges

Who is this course for?

Ideal for newcomers to cybersecurity, IT professionals, and anyone looking to build a solid foundation in the field. Great for organizations looking to train new teams or upskill other departments.

CONSPECT:

Basic knowledge

- Common course part, knowledge and skills required during rest of course modules.
  - Linux Basics
  - Windows Basics
  - Networking Fundamentals

PEN-100 Network Penetration Testing Essentials

- Network Penetration Testing Essentials module is designed to prepare learners to begin their penetration testing journey. This learning path covers the main concepts of information security such as cryptography, scripting, networking protocols, and working with shells. Interns, system administrators, developers, and other information technology professionals will get exposed to cybersecurity-adjacent content, tools, and technology needed to begin learning penetration testing skills. After completing the Network Penetration Testing Essentials learning path, learners will have earned the essential skills and confidence to pursue advanced material, namely the Penetration Testing with Kali Linux (PEN-200) course.
  - Cryptography
  - Web Applications
  - Introduction to Active Directory
  - Working w/ Shells
  - Bash, Python and PowerShell Scripting
  - Troubleshooting

WEB-100 Web Application Assessment Essentials

- The Web Application Assessment Essentials module is designed to help Learners grasp the basics needed to start learning web application security. Web Application Assessment Essentials covers tech-adjacent concepts that are pillars for any cybersecurity focus area and are valuable for upskilling technical professionals to security roles. The module also covers web

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

app security-specific Learning Modules such as Secure Coding, Web Attacker Methodology, and Input Validation. Hands-on Learning Module Exercises allow Learners to practice and solidify their skills. Learners who complete Web Application Assessment Essentials will gain the necessary knowledge to enroll in the Web Attacks with Kali Linux (WEB-200) course.

- Web Attacker Methodology
- Web Applications
- Introduction to Web Secure Coding
- JavaScript Basics
- Input Validation
- Web Session Management

EXP-100 Exploit Development Essentials

- Exploit Development Essentials is an introductory-level Learning Path. It provides Learners with the knowledge and skills necessary to learn exploit development. Learners will acquire knowledge of information security and skills needed for learning exploit development with Learning Modules such as Intro to Intel Assembly, Intro to ARM, and Intro to WinDbg. By completing this Learning Path, Learners will be ready to take on training to gain more advanced exploit development skills and certifications. Exploit Development Essentials is designed to equip Learners with the necessary knowledge to enroll in the Windows User Mode Exploit Development (EXP-301) course.
  - Intro to Intel Assembly
  - Intro to Intel Assembly II
  - Intro to ARM
  - Intro to ARM II
  - Intro to WinDbg
  - Intro to Analysis with IDA Pro

SOC-100 Security Operations Essentials

- The Security Operations Essentials Learning module introduces learners to the cybersecurity defense and security operations essentials. Security Operations Essentials is an ideal prelude to the Security Operations and Defensive Analysis (SOC-200) course.
  - Linux Networking and Services
  - Enterprise Network Architecture
  - SOC Management Processes
  - Windows Networking and Services
  - Introduction to Active Directory
  - Troubleshooting

CLD-100 Introduction to Cloud Security

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Introduction to Cloud Security is designed for individuals and organizations to start working towards a specialization in cloud security. This Learning Path is vendor-agnostic and provides real-world content on the underlying security concepts of cloud computing that can be applied to any cloud vendor: Amazon Web Services, Google Cloud, or Microsoft Azure. Learners will be equipped with knowledge and skills in cloud security Learning Modules such as Kubernetes, Containers, and Cloud Architecture. These skills will empower you or your team to build secure cloud-native applications and drive secure cloud implementations.
  - Introduction to Cloud Security
  - Containers for Cloud
  - Introduction to Kubernetes I
  - Discovering Exposed Docker Sockets
  - Discovering Exposed Kubernetes Dashboards

SSD-100 Introduction to Secure Software Development

- Introduction to Secure Software Development is a hands-on Learning Path that teaches developers and security professionals how to implement security concepts throughout software development lifecycles. Through a combination of content on language-agnostic secure coding principles, videos, and practical exercises, every development team will build skills applicable to a broad range of web technologies. Introduction to Secure Software Development is ideal for roles such as Security Software Engineer, Applications Engineer, Release Manager, Software Developer, or anyone committed to the defense or security of enterprise applications. Completing this Learning Path will empower developers to build and deploy secure software from the start to prevent vulnerabilities, and security professionals will gain an understanding of the software development process.
  - Introduction to Secure Software Development
  - Introduction to SQL Injection
  - Introduction to Web Application Debugging
  - Secure Development Lifecycle

Bonus parts of the course available in the form of self-study digital content PEN-103 and PEN-210

- PEN-103 Kali Linux Reinvented (+ 1 KLCP exam attempt)
  - This course covers everything you need to know to be able to effectively use and deploy Kali Linux. This course will discuss basic Linux usage for beginners, Debian package management and usage, Kali installation, configuration, security, and advanced Kali usage including how Kali fits within the enterprise and Kali's role in various phases of a security assessment. This course supports the Kali Linux Certified Professional (KLCP) certification. Benefits:
    - Use & Deploy Kali Linux in enterprise environments
    - Improve and polish your control of Kali Linux, unlocking the full distribution potential
  - PEN-210 Foundational Wireless Network Attacks (+1 OSWP exam attempt)

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Wireless Attacks (PEN-210) introduces learners to the skills needed to audit and secure wireless devices and is a foundational course alongside PEN-200 and benefits those who would like to gain more skills in network security. Learners will identify vulnerabilities in 802.11 networks and execute organized techniques and those who complete the course and pass the exam will earn the OffSec Wireless Professional (OSWP) certification. Benefits:
  - Be able to identify existing encryptions and vulnerabilities in 802.11 networks
  - Circumvent network security restrictions and recover the encryption keys in use

REQUIREMENTS:

No prior cybersecurity experience is required. While some IT background can be beneficial, the learning path is designed to introduce fundamental cybersecurity concepts, making it accessible to all.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

During OffSec Security Fundamentals you will have possibility to check your progress and the level of preparedness with assessments and possibility to gain badges.

The OffSec Security Fundamentals course and included bonus parts PEN-103 and PEN-210 prepares to the Kali Linux Certified Professional (KLCP) certification exam https://help.offsec.com/hc/en-us/articles/360059125211-KLCP-Exam-Guide and the OffSec Wireless Professional (OSWP) certification exam https://help.offsec.com/hc/en-us/articles/360046904731-OSWP-Exam-Guide

Each participant in an authorized OffSec Security Fundamentals training held in Compendium CE will receive a free 1 KLCP exam attempt and 1 OSWP exam attempt.

TRAINER:

Authorized OffSec Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

ADDITIONAL INFORMATION:

The course includes a license “Learn Fundametals”.

The license includes:

- 1 year of unlimited access to all OffSec fundamental content **https://www.offsec.com/products/fundamentals/**
- 365 days of lab access
- PEN-103 + 1 KLCP exam attempt
- PEN-210 + 1 OSWP exam attempt

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007