800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

OffSec Learn Fundamentals Training

OffSec Authorized Training · Applied Technology Academy

OffSec Learn Fundamentals Training from Applied Technology Academy — live online, classroom and private team delivery.

PEN: Network Penetration Testing Essentials

Network Penetration Testing Essentials is a learning path 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.

The Network Penetration Testing Essentials Assessment and Badge enables individuals and organizations to track their progress and understand the level of assimilated content. 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.

By completing the Network Penetration Testing Essentials Learning Path, Learners will:

- Obtain basic IT and information security skills
- Get prepared to advance their skills and enroll in PEN-200: Penetration Testing with Kali Linux
- Start their preparation for entry-level security roles
- Test their progress and the level of preparedness with Assessments and Badges
- Learning Module Examples
- Linux Basics
- Windows Basics
- Networking Fundamentals
- Cryptography
- Web Applications
- Introduction to Active Directory
- Working w/ Shells
- Bash, Python and PowerShell Scripting
- Troubleshooting

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

WEB: Web Application Assessment Essentials

The Web Application Assessment Essentials learning path 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 training also covers web 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.

By completing the Web Application Assessment Essentials Learning Path, Learners will:

- Keep track of their progress with interactive exercises throughout the Learning Path
- Get challenged to perform with security in mind
- Test their progress and the level of preparedness with Assessments and Badges
- Elevate their skill set in web application security and prepare for advanced training and certifications
- Learning Module Examples
- Linux and Windows Basics
- Networking Fundamentals
- Web Attacker Methodology
- Web Applications
- Introduction to Web Secure Coding
- JavaScript Basics
- Input Validation
- Web Session Management

SOC: Security Operations Essentials

The Security Operations Essentials Learning Path introduces Learners to the cybersecurity defense and security operations essentials. With more than 10 extensive Learning Modules as well as hands-on exercises to apply Learners' knowledge, Security Operations Essentials will help you or your team get familiar with the fundamental processes and methodologies needed to start learning security operations and defense.

To demonstrate their skill level and learning journey, Learners can take Assessments and earn OffSec Badges. Security Operations Essentials is an ideal prelude to the Security Operations and Defensive Analysis (SOC-200) course where Learners can train and get certified for roles such as SOC Junior Analyst and Threat Hunter.

By completing the Security Operations Essentials Learning Path, Learners will:

- Get equipped with introductory cyber defense training

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- Be able to track their journey with practical Learning Module Exercises
- Prepare to enroll in SOC-200: Foundational Security Operations and Defensive Analysis
- Test their progress and the level of preparedness with Assessments and Badges
- Learning Module Examples
- Linux Basics
- Windows Basics
- Networking Fundamentals
- Linux Networking and Services
- Enterprise Network Architecture
- SOC Management Processes
- Windows Networking and Services
- Introduction to Active Directory
- Troubleshooting

EXP: 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.

By completing the Exploit Development Essentials Learning Path, Learners will:

- Get introduced to the essentials of exploit development
- Keep track of their learning journey and the level of assimilated knowledge through hands-on exercises
- Test their progress and the level of preparedness with Assessments and Badges
- Be prepared to take on more advanced exploit development learning and courses
- Learning Module Examples
- 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

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

CLD: Introduction to Cloud Security

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.

By completing the Introduction to Cloud Security Learning Path, Learners will:

- Boost their fundamental knowledge of cloud security
- Get a head start in learning toward a successful career in the field
- Be prepared to understand higher-level cybersecurity content
- Keep track of their learning progress through interactive, hands-on exercises
- Learning Module Examples
- Introduction to Cloud Security
- Containers for Cloud
- Introduction to Kubernetes I
- Discovering Exposed Docker Sockets
- Discovering Exposed Kubernetes Dashboards

SSD: 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.

By completing the Introduction to Secure Software Development Learning Path, Learners will:

- Become immersed in secure software development
- Learn how to write secure code and avoid common bugs and vulnerabilities
- Enrich their DevOps and DevSecOps skills with secure coding principles
- Create a security-first mindset through practical exercises

- Learning Module Examples
- Introduction to Secure Software Development
- Introduction to SQL Injection
- Introduction to Web Application Debugging
- Secure Development Lifecycle

OWASP Top 10:2021

The OffSec OWASP Top 10 Learning Path is a valuable fundamental level training for professionals expanding their expertise in application security. This Learning Path, independent of specific platforms, focuses on the most pressing security vulnerabilities, applicable universally in the digital space.

By completing the OWASP Top 10:2021 Learning Path, Learners will gain:

- A foundational grasp of the most critical application vulnerabilities, as outlined by OWASP.
- Familiarity with common attack vectors and effective mitigation strategies.
- Practical know-how for identifying and rectifying security flaws in software systems.
- Techniques for proactive application security practices and risk assessment.
- Learning Module Examples
- A01:2021 – Broken Access Control
- A02:2021 – Cryptographic Failures
- A03:2021 – Injection
- A04:2021 – Insecure Design

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.