SEC275: Foundations: Computers, Technology, & Security

Course Overview

SANS Foundations is the most comprehensive, certified introductory cybersecurity course on the market. It supports your early steps into the industry by enabling you to master the fundamental knowledge and demonstrate the practical skills you need to prove you are ready for that first job in cybersecurity.

SANS instructors developed SANS Foundations to help you learn in a way that works best for you. Our engaging, high-definition video lectures are supported by audio recordings, hands-on labs and exercises, ensuring every student graduates with real-world, practical skills.

The course covers the foundations of cybersecurity in 12 modules, they are:

- Computer Components and Concepts
- Linux
- The Web
- Networking Fundamentals
- Servers and Services
- Practical Programming and Concepts
- SQL
- Windows Foundations
- Advanced Computer Hardware
- Security Concepts
- Offensive Security Concepts
- Network and Computer Infiltration

Job Roles

- Network Forensics Cybersecurity Analyst
- Senior Cybersecurity Engineer
- Network Vulnerability Assessor
- Penetration Tester Consultant
- Cybersecurity Engineer
- Cybersecurity Auditor

Who Should Attend:

- Career changers
- Online, self-driven learners seeking new skills
- College & university students
- Business professionals without a deep cybersecurity background
- New hires in IT/cybersecurity
- Participants in reskilling program

Prerequisites

There are no prerequisites.

No prior security knowledge is needed.

Duration

6 Days

Certifications

GIAC Foundational Cybersecurity Technologies (GFACT)

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

LDR551: Building and Leading Security Operations Centers

APPLIED TECHNOLOGY ACADEMY

Course Outline

Overview

The syllabus is expertly curated to progressively take students from no technical, or security knowledge, to a level where they are speaking the same language as industry professionals.

Topics

- Introduction
- Computer Components and Concepts
- Linux
- The Web
- Networking Fundamentals
- Servers and Services
- Practical Programming and Concepts
- SQL
- Windows Foundations
- Advanced Computer Hardware
- Security Concepts
- Offensive Security Concepts
- Network and Computer Infiltration

Course Summary

The summary refreshes the memory as it reviews all the course material and prepares the student for the final GFACT (GIAC Foundational Cybersecurity Technologies) exam.

Course Objectives

- Understand key hardware components and associated memory concepts
- Understand the uses of virtualization and containers, with their advantages, and disadvantages.
- Be familiar with common exploit anatomy, methodology, and the tools used by attackers
- Be familiar with tools used in forensics investigations and their function.
- Have a working knowledge of most used Linux commands, permissions, and access control
- Understand core networking concepts, protocols, different server types and their uses.
- Be able to determine the result of basic logical operation.
- Be familiar with programming syntax, constructs, and errors in popular languages.
- Recognise different file systems, web technology, and cloud computing models.
- Be comfortable with the concepts and terminology associated with cryptography
- Be familiar with the ethical and legal concerns associated with hacking
- Know the stages of an attack and be familiar with key defensive strategies and concepts.
- Be familiar with key Windows CLI commands, permissions and access control.

Foundational Cybersecurity Technologies (GFACT)

The GIAC Foundational Cybersecurity Technologies (GFACT) certification validates a practitioner's knowledge of essential foundational cybersecurity concepts. GFACT-certified professionals are familiar with practical skills in computers, technology, and security fundamentals that are needed to kickstart a career in cybersecurity.

- Core Computing Components: Hardware and Virtualization, Networking, Operating Systems, Web, Cloud, and Data Storage
- IT Fundamentals and Concepts: Logic and Programming, Windows, and Linux
- Security Foundations and Threat Landscape: Concepts, Exploitation and Mitigation, Forensics and Post Exploitation