SEC275:™ Foundations: Computers, Technology and Security™

GFACT
Foundational Cybersecurity Technologies
giac.org/gfact

Online Course | 38 CPEs | Laptop Required

You Will Be Able To

- 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.
- Recognize 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

What is Included

- 90+ embedded labs to practice skills in real-life environment
- 55+ quizzes to capture learning outcomes
- 190+ video lectures and walk through demonstrations
- Audio guidance throughout all sections of the course
- Proctored final exam delivered by GIAC

SANS Foundations™ is the most comprehensive, certified introductory cybersecurity course on the market. Developed by leading subject matter experts, SEC275 training provides fundamental cybersecurity knowledge and skills, giving students with no prior technical or industry experience a level of proficiency that allows them to speak the same language as professionals. Learn foundational computer and security concepts and develop programming skills in an interactive learning environment, supported by world-renowned instructors, video lectures, hands-on labs and exercises.

SANS Foundations™ transforms learning into real-world, practical skills, going far beyond what all other foundational cybersecurity courses offer.

Who is the SANS Foundations course for?

Whether you're new to cybersecurity, a career changer, or an experienced IT professional looking to revise the fundamentals, SANS Foundations™ is the perfect introduction for those exploring a technical career in cybersecurity.

Authors' Statements

"The landscape of cybersecurity is changing rapidly and constantly evolving. There are new threats emerging daily, new attackers using novel techniques, and worryingly, a growing shortage of global talent.

Before running to the exciting worlds of application security, reverse malware engineering or threat hunting, every cybersecurity professional needs to have an excellent grounding in essential computing and technology skills. These will be used every day in your career and serve as a baseline for your development and future career.

"SANS Foundations™ is the most comprehensive, certified introductory cybersecurity course on the market. We wanted to make this course as accessible as possible, to eradicate as many potential hurdles stopping people getting into the field. We've specifically designed the course to require minimal equipment or technology proficiency—you do not need any prior specific education, just a keen interest.

"Whether you are still in full-time education, a career changer or on an immersive training program, SANS Foundations™ will provide you with the core IT and computer knowledge integral to a future, technical career in cybersecurity."

—James Lyne, SANS Chief Technology and Innovation Officer

"Cybersecurity can feel overwhelming at the start. New tools, new threats, and a lot of assumed knowledge before you ever touch a keyboard.

SANS Foundations exists to change that.

This is a technical introductory course, not a computer science degree and not an advanced deep dive into specialties like threat hunting or reverse engineering. Instead, it introduces the essential computing, networking, operating system, and security concepts that various cybersecurity professionals rely on every day.

The goal is confidence, not mastery. Confidence to understand what is happening under the hood, to ask better questions, and to take your next steps with clarity instead of guesswork.

You do not need prior technical training or specialized equipment. Just curiosity and a willingness to learn how systems actually work.

Whether you are a student, a career changer, or exploring cybersecurity for the first time, this course gives you the foundation to move forward with purpose."

—Rich Greene, SANS Certified Instructor

Syllabus

Introduction
Learning the Foundations—This module introduces the SANS Foundations course and training platform, including how to use the product.

1. Computer Components and Concepts
This module focuses on the different components of a computer, what they do, and how they work together. It covers topics such as computer hardware, data storage and representation, logic and data manipulation, storing data and files, cloud computing, operating systems, and virtualization.

2. Linux
This module introduces students to Linux, including the Linux environment, navigation, commands, and architecture. Topics include installing Linux, navigation and structure, permissions, and commands like grep, cp, and more. It's lab-intensive allowing students to practice skills hands-on.

3. The Web
This module covers the fundamentals of how search engines work, effective search techniques, web servers, HTML, and cookies.

4. Networking Fundamentals
Students learn core networking concepts, including networking components and hardware, packets, network addresses, TCP and UDP protocols, subnetting, and email.

5. Servers and Services
This module covers different server types, such as web, database, DNS, log, and email servers, including basic setup and installation. It also explores cloud computing, configuration, and hardening basics.

6. Practical Programming and Concepts
An introduction to programming in Python and C, this module covers programming fundamentals and hands-on exercises in Python and C, with labs on topics like variables, user input, file handling, TCP sockets, and more.

7. SQL
This module introduces SQL basics, including statements, joins, operators, and database administration, laying groundwork for offensive security concepts later in the course.

8. Windows Foundations
This module covers essential Windows CLI commands, permissions, file systems, architecture, networking, and PowerShell. Students learn setup, configuration, logging, registry, user accounts, and more.

9. Advanced Computer Hardware
This module delves into how CPU and RAM functions, and covering advanced storage (e.g., RAID, cloud storage).

10. Assembly
This module is an introduction to basic assembly, debugging and reverse engineering using GDB.

11. Security Concepts
This module introduces cryptography and ethical/legal concerns in hacking. Topics include encryption, encoding, hashing, ethics, risk management, reconnaissance tools, and digital forensics.

12. Offensive Security Concepts
This module covers exploitation techniques such as command injection, SQL injection, session guessing, directory traversal, and more. Tools like Metasploit and techniques for privilege escalation and social engineering are also introduced.

13. Network and Computer Infiltration
This module covers persistence, lateral movement, and exfiltration. Students learn about indicators of compromise, ARP cache, rootkits, and common exfiltration methods.

Further Study
The summary reviews all course material, preparing students for the GIAC Foundational Cybersecurity Technologies (GFACT) exam.

"The security labs were my personal favorite as the skills attained through those helped me land a role as a vulnerability analyst in the information security office!"

—Kirti Nangia, **SANS Foundations Student**

Who should take SANS Foundations?
- Career changers
- Self-driven learners seeking new skills online
- College and university students
- Business professionals working in IT or cybersecurity
- New hires in IT/cybersecurity
- Participants in reskilling and retraining programs

GFACT
Foundational Cybersecurity Technologies
giac.org/gfact

GIAC Foundational Cybersecurity Technologies
The 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

"The GFACT certification prepared me for the GIAC Security Essentials (GSEC) exam, equipping me with the necessary knowledge and skills. Beyond certification, the course established a strong foundation for continuous learning and professional development in cybersecurity. This has set the stage for my goal of pursuing additional certifications and expanding my expertise over the next 10–20 years."

—Norzaini Elias, **SANS Foundations Student**