SEC275: Foundations: Computers, Technology and Security

GFACT
Foundational Cybersecurity Technologies
giac.org/gfact

Online Course | 38 CPEs | Laptop Required

What You Will Learn

You'll be taken through the 12 modules below, covering the foundations of IT, technology and security, taking you to a level of proficiency where you'll be speaking the same language as professionals. No prior technical experience required.

- Computer Components and Concepts
- Linux
- The Web
- Networking Fundamentals
- Servers and Services
- Practical Programming and Concepts
- SQL
- Windows Foundations
- Advanced computer software
- Security concepts
- Offensive Security Concepts
- Network and Computer infiltration

To help build on your newfound knowledge, you will practice using the Linux command line, writing computer programs in C and Python, and running common exploits in hands-on labs and exercises included in the course.

The labs draw on the latest technology, techniques, and concepts in cybersecurity, bringing your knowledge to life in a practical, technical environment, giving you real-world skills that prepare you for the first day of your new cybersecurity career.

What is included with SANS Foundations?

- 60+ embedded labs
- 55+ quizzes to track your progress
- 145+ video lectures and walk through demonstrations
- 200+ audio recordings guiding students through course material
- 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 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.

Author Statement

"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

"The security labs were my personal favourite 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**

"Despite having a senior level security role SANS Foundations was a fantastic way to brush up on important concepts that help me better fulfill my job duties."

— Noah Pack, **SANS Foundations Student**

Syllabus

Introduction:

Learning the Foundations – introduction to the SANS Foundations course.

1. **Computer Components and Concepts:**

   This module focuses on the different components of a computer, what they do, and how they work together. It looks at Computer Hardware, Data Storage & Representation, Logic & Data Manipulation, Storing Data & Files, Cloud Computing, Operating Systems and Virtualization.

2. **Linux:**

   This module introduces students to Linux, the Linux Environment, Linux Navigation, Commands, and Linux Architecture and Components. These subjects help students develop a working knowledge and understanding of installing Linux, navigation and structure, permissions, and commands such as grep, cp, and much more. This module is rich in labs to helps students practice their skills.

3. **The Web:**

   This module provides a look into how search engines work, and the most efficient ways to use them, as well as introducing web servers, HTML and cookies.

4. **Networking Fundamentals:**

   This module helps students understand core networking concepts and protocols including networking components and hardware, packets, types of network addresses, TCP and UDP protocols, subnetting, and email.

5. **Servers and Services:**

   This module helps students understand the different server types by introducing web, database, DNS (Domain Name System), Log, and Email servers; looking at their basic setup and installation procedures. The module covers basic hardening and configuration and concludes with a deep dive into Cloud Computing.

6. **Practical Programming and Concepts:**

   The module is a student's first look at programming in Python and C. The sections incrementally teach what a program is and how it works, before delving into writing basic programming, and introducing various strategies, tools, and conventions. These sections are lab-heavy, including labs such as variables in python, user input in python, reading and writing files, using TCP sockets, printing in C, string handling, and more!

7. **SQL:**

   This module teaches students about basic statements, joins, operators and database admins. Learning the fundamentals of SQL will help prepare students for more Offensive Security Concepts work later in the course.

8. **Windows Foundations:**

   The Windows Foundations module helps students get familiar with key Windows CLI commands, understanding permissions and access control, and elements of Windows as it relates to file systems, architecture, and networking. This module also looks at Windows uses, installation, network setup, configuration, changing settings, log files, the registry, file permissions, user accounts, Windows command line, scripting, and Powershell.

9. **Advanced Computer Hardware:**

   The Advanced Computer Hardware module looks at how the CPU and RAM work in depth (e.g., Memory: Stack and Heap). It introduces, and looks at GDB in practice, along with how to track execution, with advanced storage mechanisms such as RAID and cloud storage mechanisms. The module also covers an introduction into Assembly, and it explores mnemonics.

10. **Security Concepts:**

    This module introduces students to the concepts and terminology associated with cryptography, whilst becoming familiar with the ethical and legal concerns associated with hacking. They cover a variety of topics and tools such as encryption, encoding, hashing, the law, ethics, red teams vs. blue team, risk management, critical security controls, Kali Linux, Slingshot and SIFT, reconnaissance tools and techniques, and the basics of digital forensics (e.g., steganography, memory captures).

11. **Offensive Security Concepts:**

    This module introduces students to offensive security concepts and exploitation techniques, such as command injection, SQL injection, session guessing, directory traversal, clickjacking, buffer overflows, phishing, Metasploit, social engineering, privilege escalation, kernel exploits, bypassing UAC, stored credentials, and more!

12. **Network and Computer Infiltration:**

    This module covers topics and methods for persistence, lateral movement, and exfiltration. Students learn about indicators of compromise, ports, Yara, Rootkits, ARP Cache, extracting passwords from memory, spotting common exfiltration methods, and more.

Course Summary:

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

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
- Participants in federal or government training programs
- Participants in business or enterprise apprenticeships

GFACT

Foundational Cybersecurity Technologies

giac.org/gfact

GIAC Foundational Cybersecurity Technologies

"The GIAC Foundational Cybersecurity Technologies (GFACT) certification demonstrates an individual has developed hands-on skills through labs in areas such as Linux, encryption, and programming, as well as gained essential knowledge in areas such as networking, computer hardware, virtualization, Windows, servers, introductory security concepts, and more. Candidates achieving the GFACT are proficient in the core knowledge and practical skills in computers, technology, and security fundamentals needed to kickstart a career in cybersecurity. GFACT holders are truly ready to contribute on Day 1 of their first job in IT or cybersecurity!"
—**James Lyne, SANS Chief Technology and Innovation Officer**

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