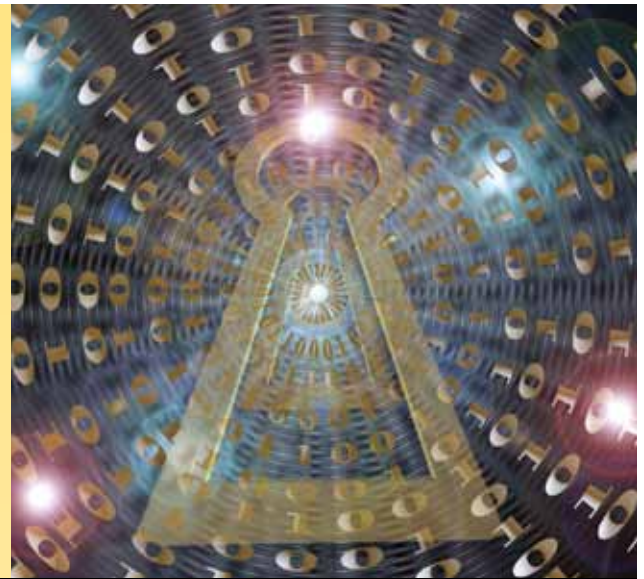


SEC401: SANS Security Essentials Bootcamp Style

Course Length: Six Days • 46 CPE Credits
Laptop Required

Security Essentials is designed to give anyone interested in network security the skills required to be an effective player in this space. This in-depth, comprehensive course provides the essential, up-to-the-minute knowledge and skills required for securing systems and organizations and equips you with the language and theory of computer security. Learn all of this and more from the best security instructors in the industry.



Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification.

B O O T C A M P

Security 401 PARTICIPANTS ONLY

5:15pm - 7:00pm - **Required** — Course Days 1-5

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "cookbook for geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study, and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.

This course prepares you for the IAT Level II of the Department of Defense Baseline Certification for 8570

Security Curriculum

SEC301
Intro to Information
Security
GISF

SEC301 NOTE:

If you have experience in the field, please consider our more advanced course – SEC401.

SEC401
SANS Security Essentials
Bootcamp Style
GSEC

SEC501: Advanced Security Essentials - Enterprise Defender

SEC502: Perimeter Protection In-Depth

SEC503: Intrusion Detection In-Depth

SEC504: Hacker Techniques, Exploits & Incident Handling

SEC505: Securing Windows

SEC506: Securing Linux/Unix

SEC509: Securing Oracle

SEC540: VoIP Security

SEC542: Web App Penetration Testing & Ethical Hacking

SEC560: Network Penetration Testing & Ethical Hacking

AUD507: Auditing Networks, Perimeters & Systems

MGT414: SANS® + S™ Training Program for the CISSP® Certification Exam

MGT525: Project Management & Effective Communications for Security Professionals and Managers



www.sans.org

For more information, visit <http://www.sans.org>

When registering, use this promo code **SEC401**

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Network engineers wanting to enter the field of security
- Security engineers, admins, managers, and others wanting a more detailed understanding of the technical components of security
- Anyone new to information security with some background in information systems and networking
- Individuals with operational responsibility for a firewall, VPN, or Internet-facing device

Author Statement

One of the things I love to hear from students after teaching Security 401 is, "I have worked in security for many years, and after taking this course I realized how much I did not know." With the latest version of SANS Security Essentials Bootcamp Style, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After attending this course, I am confident you will walk away with solutions to problems you have had for a while plus solutions to problems you did not even know you had. -Eric Cole, PhD

Sampling of Course Topics

- Risk Assessment and Auditing
- Host and Network Based Intrusion Detection
- Honeypots, Firewalls and Perimeter Protection
- Security Policy
- Password Management
- Security Incident Handling - The Six Steps
- Information Warfare
- Web Security
- Network Fundamentals and IP Concepts and Behavior
- Cisco Router Filters
- Four Primary Threats for Perimeter Protection
- PGP, Steganography
- Anti-Viral Tools
- Windows (2000, XP, 2003, Vista) Security Administration and Auditing
- IIS Security
- Unix Security Fundamentals



GIAC Security Essentials Certification (GSEC)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

Four Reasons to 'Get GIAC Certified'

GIAC Certification:

- 1 Promotes** learning that improves your hands-on technical skills and improves knowledge retention
- 2 Provides** proof that you possess hands-on technical skills
- 3 Positions** you to be promoted and earn respect among your peers
- 4 Proves** to hiring managers that a candidate is qualified for the job

**Learn more about GIAC at
www.giac.org.**

**Test your security knowledge with our
SANS Security Essentials Assessment Test.
Get your free test at
<https://portal.sans.org/assessments/>**