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 and managers or others want 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

Laptop required

GIAC Certification
You may register to seek certification for an additional fee of $400 US.
For more information go to the GIAC home page www.giac.org and the GIAC FAQ www.giac.org/faq.php.

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.

In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential knowledge and skills required for effective performance if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work and (2) You will be taught by the best security instructors in the industry. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a competition among potential security faculty.

BooT CAMP

Security 401 PARTICIPANTS ONLY
5:15pm - 7:00pm - Required — Course Days 1-5

Attendance is required for the evening Bootcamp sessions (each evening for days 1-5) as the information presented appears on the GIAC Exams. The material covered in these sessions is based on Eric Cole's "cookbook for geeks" and most students find Bootcamp to be the highlight of their Security Essentials experience! Apply the knowledge gained throughout the course in an instructor-led environment. 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 that has both a Red Hat 9.0 partition and a Windows XP partition. A working knowledge of each operating system is recommended but not required to get a great deal of knowledge from the course. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

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

Please note that some course material for SEC 401 and MGT 512 may overlap. We recommend SEC 401 for those interested in a more technical course of study and MGT 512 for those primarily interested in a leadership-oriented but less technical learning experience.
Security Essentials is our most popular training program. We strongly recommend you attend the evening bootcamp sessions with hands-on exercises. These require the dedication to really put in the hours, but they can help you fill in the gaps in your information security knowledge. Everyone, except truly seasoned hands-on information security workers, can benefit from SANS Security Essentials Bootcamp Style. A GSEC Certification can add 6-9% to your bottom line salary.

401.1 Hands-On – SANS Security Essentials I: Networking Concepts
A key way attackers gain access to a company’s resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine hostile traffic. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials and more will be covered to provide a firm foundation for the consecutive day’s training.
Topics: Network Fundamentals; IP Concepts; IP Behavior; Routing Fundamentals; Safety & Physical Security; Voice over IP (VoIP)

401.2 Hands-On – SANS Security Essentials II: Defense-In-Depth
In order to secure an enterprise network, you must have an understanding of the general principles of network security. In this course you will learn about six key areas of network security. The day starts with information assurance foundations where students learn about both current and historical computer security threats and how they impact computer security, integrity, and availability. The first half of the day also covers the instruction for creating sound security policies and password management, including tools for password strengths on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at what can be done to test and protect a Web server in your company.
Topics: Defense-In-Depth; Basic Security Policy; Access Control & Password Management; Information Warfare; Web Communications & Security

401.3 Hands-On – SANS Security Essentials III: Internet Security Technologies
Military agencies, banks and retailers offering electronic commerce programs, and dozens of other types of organizations are demanding to know what threats they are facing and what they can do to alleviate those threats. In this course you will obtain a roadmap that will help you understand the paths available to organizations that are considering or planning to deploy various security devices and tools, such as intrusion detection systems and firewalls. The course goes beyond the narrow technical view and offers a full context for the deployment of these promising new technologies. When it comes to securing your enterprise, there is no single technology that is going to solve all of a company’s security issues. However, by implementing an in-depth defense strategy that includes multiple defensive measures, you can go a long way in securing your enterprise. Each section in this course covers one tool that will play a part in a company’s overall information assurance program.
Topics: Host-based Intrusion Detection and Prevention; Network-based Intrusion Detection and Prevention; Honeypots; Methods of Attacks; Firewalls and Perimeters; Risk Management

401.4 Hands-On – SANS Security Essentials IV: Secure Communications
There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies use it. This technology is encryption. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day four looks at various aspects of encryption and how it can be used to secure a company’s assets. A related area called steganography, or information hiding, is also covered. Wireless is becoming a part of most modern networks but it is often implemented in a non-secure manner. Security issues associated with wireless and what can be done to protect these networks will also be discussed. This section finishes by tying all of the other pieces together through a look at operations security.
Topics: Cryptography; Steganography; Encryption; PGP; Wireless; Operations Security

401.5 SANS Security Essentials V: Windows Security
Windows is the most widely-used and hacked operating system on the planet, and Internet Explorer is every hacker’s “favorite” browser. The simple days of Windows 98 desktops and Windows NT 4.0 domains are long gone, replaced by the complexities of Active Directory, Group Policy, PKI, BitLocker, etc. This section will help you to quickly master the world of Windows security while showing you the tools you can use to simplify and automate your work. You will complete the day with a solid grounding in Windows security, including the important new features in Windows Vista.
Topics: The Security Infrastructure; Permissions and User Rights; Security Policies and Templates; Service Packs, Patches, and Backups; Securing Network Services; Auditing and Automation.

401.6 SANS Security Essentials VI: Unix Security
Based on industry consensus standards, this course provides step-by-step guidance on improving the security of any Unix operating system. The course combines practical how-to instructions with background information for Unix beginners and security advice and best practices for administrators of all levels of expertise.
Topics: Patching and Software Management; Minimizing System Services; Logging & Warning; Access Control; Security Configuration; Backups and Archives