SEC401: **Security Essentials Bootcamp Style**

GSEC
Security Essentials
giac.org/gsec

6	46	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark

> **“SEC401 is a great intro and overview of network security. It covered just enough information to get a baseline level of knowledge without going too in-depth on any one topic.”**
>
> — Josh Winter, **Washington County, MN**

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

- Do you fully understand why some organizations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, then SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. Our course will show you how to prevent your organization’s security problems from being headline news in the *Wall Street Journal*!

Prevention is ideal but detection is a must.

With the rise in advanced persistent threats, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organization’s network depends on the effectiveness of the organization’s defense. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organizations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

- What is the risk?
- Is it the highest priority risk?
- What is the most cost-effective way to reduce the risk?

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need 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 learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Network Security Essentials

A key way that 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 and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered in this first section in order to provide a firm foundation for the consecutive sections of training.

TOPICS: Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

SECTION 3: Threat Management

Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

TOPICS: Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/Log Management; Active Defense

SECTION 5: Windows Security

Remember when Windows was simple? Windows XP desktops in a little workgroup...what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the section with a solid grounding in Windows security by looking at automation, auditing and forensics.

TOPICS: Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

SECTION 2: Defense-In-Depth and Attacks

To secure an enterprise network, you must understand the general principles of network security. In Section 2, we look at threats to our systems and take a "big picture" look at how to defend against them. You will learn that protections need to be layered – a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

TOPICS: Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

SECTION 4: Cryptography, Risk Management, and Response

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 deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. This course section 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.

TOPICS: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

SECTION 6: Linux Security

While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course section provides step-by-step guidance to improve the security of any Linux system. The course combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

TOPICS: Linux Security: Structure, Permissions and Access; Hardening and Securing Linux Services; Monitoring and Attack Detection; Security Utilities

Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

"SEC401 provided a vast library of information on developing a strong security posture, and in the course of the training my brain shifted into a security-first gear thanks to the intense and deep exposure to the multitudinous recommendations for securing an organization's network and data."

— Laura Farvour,
University of Minnesota

Course Preview
available at: **sans.org/demo**