12 Appendix A: Course Overview

12.1 SEC401: Security Essentials Bootcamp Style

Hands On | Six Days | Laptop Required | 46 CPE/CMU Credits | GIAC Cert: GSEC

SEC401 focusses on teaching the steps necessary to prevent attacks and to detect adversaries. It imparts actionable techniques that students can apply directly when they get back to work. Students who attend learn tips and tricks from the experts, equipping them with the skills needed to win the battle against a wide range of cyber adversaries. The course is built around the maxim: "Prevention is ideal but detection is a must."

With advanced persistent threats, it is almost inevitable that organisations will be targeted. Whether the attacker is successful in penetrating an organisation's network depends on the effectiveness of the organisation's defence.

Defending against attacks is an ongoing challenge, with new vectors emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cybersecurity. What has worked, and will always work, is the idea of taking a risk-based approach to cyber defence.

Before an organisation spends its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:
1. What is the risk?
2. Is it the highest priority risk?
3. What is the most cost-effective way to reduce the risk?

Security is all about making sure businesses focus on the right areas of defence. In SEC401, students learn the language and underlying theory of computer and information security. The courses teaches essential and effective security knowledge. It also equips defenders who have been given responsibility for securing systems with the skills needed to success.

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.

You Will Be Able To:

- Design and build a network architecture using VLAN's, NAC and 802.1x based on an APT indicator of compromise
- Run Windows command line tools to analyse 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 organisation and prepare a checklist to validate security, creating metrics to tie into training and awareness
- Identify visible weaknesses of a system utilising various tools to include dumpsec and OpenVAS, and once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Determine overall scores for systems utilising CIS Scoring Tools and create a system baseline across the organisation
- Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce the attack surface through hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities utilising WireShark

Hands-on Training

SEC401 is an interactive hands-on training course. The following are some of the lab activities that students will carry out:

- Setup of virtual lab environment
- Windows/Linux tutorial
- TCP dump analysis
- WireShark decoding of VoIP traffic
- Password cracking
- Host-based discovery with Dumpsec
- Hashing to preserve digital evidence

- Analyzing networks with hping and nmap
- Event correlation with Splunk
- Use of steganography tools
- Securing a Windows system with MBSA and SCA

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

Certification: GIAC Security Essentials (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.

Requirements

- 1 proctored exam
- 180 questions
- Time limit of 5 hours
- Minimum Passing Score of 74%