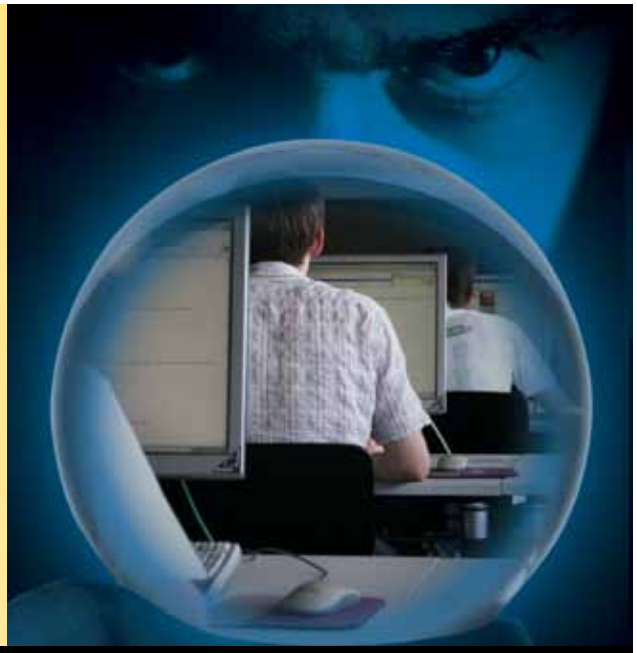
SEC504:
Hacker Techniques, Exploits, and Incident Handling

Course Length: Six Days • 36 CPE Credits
Laptop Required



From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets to the spyware your otherwise wholesome users inadvertently downloaded, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the 'oldie-but-goodie' attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. This workshop also includes the unique SANS Capture-the-Flag event on the last day where you will apply your skills developed throughout the session to match wits with your fellow students and instructor in a fun and engaging learning environment. You'll get to attack the systems in our lab and capture the flags to help make the lessons from the whole week more concrete. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

If your organization has an Internet connection or a disgruntled employee (and whose doesn't!), your computer systems will get attacked.

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

Incident Handling 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
GCED

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

FOR508
Computer Forensic Investigations and Incident Response
GCFA

Additional Incident Handling Courses

SEC517: Cutting-Edge Hacking Techniques

SEC550: Information Reconnaissance: Competitive Intelligence and Online Privacy

Who Should Attend

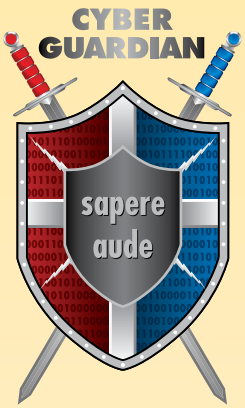
- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

A Sampling of Course Topics

- The step-by-step approach used by many computer attackers
- The latest computer attack vectors and how you can stop them
- Proactive and reactive defenses for each stage of a computer attack
- Hands-on workshop addressing scanning for, exploiting, and defending systems
- Strategies and tools for detecting each type of attack
- Attacks and defenses for Windows, Unix, switches, routers and other systems
- Application-level vulnerabilities, attacks, and defenses
- Developing an incident handling process and preparing a team for battle
- Legal issues in incident handling
- Recovering from computer attacks and restoring systems for business

Author Statement

My favorite part of teaching the Hacker Techniques, Exploits, and Incident Handling track is watching students when they finally get it. It's usually a two-stage process. First, students begin to realize how truly malicious some of these attacks are. Some students have a very visceral reaction, occasionally shouting out Oh, shoot! when they see what the bad guys are really up to. But if I stopped the process at that point, I'd be doing a disservice. The second stage is even more fun. Later in the class, students gradually realize that, even though the attacks are really nasty, they can prevent, detect, and respond to them. Using the knowledge they gain in this track, they know they'll be ready when a bad guy launches an attack against their systems. And being ready to thwart the bad guys is what its all about. -Ed Skoudis



SANS Cyber Guardian Program

SANS' Cyber Guardian program is designed for the elite teams of technical security professionals who are part of the armed forces, Department of Defense, or other government agencies whose role includes securing systems, reconnaissance, counterterrorism and counter hacks. These teams will be the cyber security special forces where each individual's role makes the team successful.

The Cyber Guardian program provides intensive, hands-on training for both Red and Blue teams. Participants must complete three core courses and the corresponding certifications within two years of starting the program. After completing all three core courses and exams, candidates will choose their specialization and complete two more courses and certifications. Upon the successful completion of all courses and certifications, candidates will finish the program by taking and passing the GSE (GIAC Security Expert) exam and joining the elite group of GSE certified professionals.

An intensive, real-world exercise on defending and attacking systems has been created to demonstrate how each cyber guardians' skills and expertise will be utilized in an actual attack.

You wouldn't go to battle with a team you have never trained with, so this exercise will show each participant how their role contributes to the success of their team.

For more information, please visit http://www.sans.org/cyber-guardian

GIAC Certified Incident Handler (GCIH)

GIAC Certified Incident Handlers have the knowledge, skills, and abilities to manage incidents; to understand common attack techniques and tools; and to defend against and/or respond to such attacks when they occur.

Target:

- **Individuals responsible for incident handling/incident response**
- **Individuals who require an understanding of the current threats to systems and networks, along with effective countermeasures**

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.