SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**

GCIH
Incident Handler
giac.org/gcih

6	37	Laptop
Day Program	CPEs	Required

You Will Learn

- How to best prepare for an eventual breach
- The step-by-step approach used by many computer attackers
- Proactive and reactive defenses for each stage of a computer attack
- How to identify active attacks and compromises
- The latest computer attack vectors and how you can stop them
- How to properly contain attacks
- How to ensure that attackers do not return
- How to recover from computer attacks and restore systems for business
- How to understand and use hacking tools and techniques
- 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
- How to develop an incident handling process and prepare a team for battle
- Legal issues in incident handling

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and one or two disgruntled employees (and whose does not!), your computer systems will get attacked. 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, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

This course enables you to turn the tables on computer attackers by helping you understand their 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. It addresses the latest cutting-edge insidious attack vectors, the “oldie-but-goodie” attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. This course will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. 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.

> **“The training offered at SANS is the best in the industry, and the SEC504 course is a must for any IT security professional – highly recommended.”**
>
> — Michael Hoffman, **Shell Oil Products US**

> **“SEC504 is the essential cert course needed to trust if a candidate is valuable enough to do incident response.”**
>
> — Troy Merritt, **Blueshield of CA**

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: Incident Handling Step-by-Step and Computer Crime Investigation

The first part of this section looks at the invaluable Incident Handling Step-by-Step Model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) necessary to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

TOPICS: Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record-Keeping; Incident Follow-Up

SECTION 2: Computer and Network Hacker Exploits – Part 1

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long section covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

TOPICS: Reconnaissance; Scanning; Intrusion Detection System (IDS) Evasion; Enumerating Windows Active Directory Targets

SECTION 3: Computer and Network Hacker Exploits – Part 2

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course section covers the third phase of many hacker attacks – gaining access. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols.

TOPICS: Physical-layer Attacks; Gathering and Parsing Packets; Operating System and Application-level Attacks; Netcat: The Attacker's Best Friend; Endpoint Security Bypass

SECTION 4: Computer and Network Hacker Exploits – Part 3

This course section starts out by covering one of attackers' favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations' homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

TOPICS: Password Cracking; Web Application Attacks; Denial of Service Attacks

SECTION 5: Computer and Network Hacker Exploits – Part 4

This course section covers the fourth and fifth phases of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens and explore future trends in malware designed to obscure an attacker's presence and disguise attribution.

TOPICS: Maintaining Access; Covering the Tracks; Putting It All Together

SECTION 6: Hacker Tools Workshop

Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

TOPICS: Hands-on Analysis

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
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

> **"I will almost always recommend SEC504 as a baseline so that everyone is speaking the same language. I want my sys-admins to take it, my network admins to take it, even my devs to take it, regardless of whether they're going to eventually move into an incident handling role. In my opinion it is the most critical, foundational class that SANS offers."**
>
> — Kevin Wilcox, **Information Security Specialist**