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

GCIH
Incident Handler
giac.org/gcih

6 Day Program | 38 CPEs | Laptop 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

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.

GCIH
Incident Handler
giac.org/gcih

GIAC Certified Incident Handler

The GIAC Incident Handler certification validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. GCIH certification holders have the knowledge needed to manage security incidents by understanding common attack techniques, vectors and tools, as well as defend against and respond to such attacks when they occur.

- Incident Handling and Computer Crime Investigation
- Computer and Network Hacker Exploits
- Hacker Tools (Nmap, Nessus, Metasploit and Netcat)

"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**

Section Descriptions

SECTION 1: Incident Handling Step-by-Step and Computer Crime Investigation

The course starts by examining the key components of both incident response and digital investigations. Informed by several incidents, we consider the goals and outcomes that are important to both business operations and security. The dynamic approach put forth can be applied to the specific needs of an individual business and incident. We then shift to more practical matters, examining issues surrounding live systems and identifying abnormal activity. Continuing the practical focus, we look at investigative techniques for examining evidence from the network and memory. We also cover techniques to determine if an unknown program is malicious, and if so, what footprints are left behind.

TOPICS: Incident Response; Digital Investigations; Live Examination; Digital Evidence; Network Investigations; Memory Investigations; Malware Investigations

SECTION 2: Recon, Scanning, and Enumeration Attacks

This course section covers the details associated with the beginning phases of many cyber attacks. We will introduce important frameworks for understanding the tools, techniques, and practices of modern attackers through the MITRE ATT&CK Framework, using it as a starting point to investigate the pre-attack steps attackers employ. We will leverage local and cloud-based tools to conduct effective reconnaissance of a target organization, identifying the information disclosure that will reveal weaknesses for initial compromise. We'll then take a deep dive into scanning techniques, both from a network perspective and with a focus on the complexities of modern Windows Active Directory forests to map out an attack plan that will grant an attacker privileged access. We will also spotlight defensive techniques using free and open-source tools that provide you with a competitive advantage to detect attacks on your organization.

TOPICS: Introducing the MITRE ATT&CK Framework; Reconnaissance; Scanning; Enumerating Windows Active Directory Targets; Defense Spotlight: DeepBlueCLI

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

SECTION 3: Password and Access Attacks

This course section starts with straightforward password guessing attacks, quickly investigating the techniques attackers employ to make this an effective process that bypasses defense systems such as account lockout. We will investigate the critical topics of creating effective password guessing lists from other network compromises, and how attackers leverage user password reuse against your organization. We'll dig into the algorithms behind password hashing, using several tools to recover plaintext passwords while optimizing the cracking process to complete in days, not years. We will also get a jump-start on understanding essential network attack topics through the use of easy backdoors, forward and reverse shells, and discrete data transfer within the organization, all through an unassuming system binary. We will also investigate defensive measures that you can immediately apply when you get back to work, including the use of the Domain Password Audit Tool (DPAT) and Elastic Stack (formerly ELK) tools for monitoring authentication logs in your organization.

TOPICS: Password Attacks; Defense Spotlight: Log Analysis with Elastic Stack (formerly ELK); Understanding Password Hashes; Password Cracking Attacks; Defense Spotlight: Domain Password Auditing; Netcat: The Attacker's Best Friend

SECTION 4: Public-Facing and Drive-By Attacks

This course section examines the hacker tools for compromising your exposed systems through exploit frameworks such as Metasploit. We also dig into the concepts and techniques behind drive-by and watering-hole attacks, and how attackers create the exploits and system-compromise tools through malicious installers, browser JavaScript, and malicious Microsoft Office documents. We'll examine the attacks specific to web applications in an organization, both from the perspective of the unauthenticated and the authenticated user, with practical exploit steps for the most popular web application vulnerabilities. In addition to examining the hacker tools, we'll also investigate several freely available and practical defense steps, including the use of the Windows SRUM database for historical system activity reporting, and the use of Elastic Stack (formerly ELK) tools for assessing web server logging data to identify signs of attack.

TOPICS: Using Metasploit for System Compromise; Drive-By and Watering Hole Attacks; Defense Spotlight: System Resource Usage Monitor (SRUM); Web Application Attacks; Defense Spotlight: Effective Web Server Log Analysis

SECTION 5: Evasion and Post-Exploitation Attacks

This course section examines the attacker steps after the initial compromise is over. We will dig into the techniques attackers use to implant malware after bypassing endpoint detection and response platforms, how they pivot through the network using third-party and built-in tools, and how they leverage the initial foothold on your network for internal network scanning and asset discovery. We will look at how the compromise of a single host grants attackers privileged network insider access to open up a whole new field of attacks, and how they will use that access wisely, covering their tracks on hosts and on the network to evade detection systems. We will look at how attackers, with their initial access established, then access, collect, and exfiltrate data from compromised networks. We will finish the lecture component of the course with a look at where to go from here in your studies, examining resources and best practices to turn your new skills into permanent, long-term recall.

TOPICS: Endpoint Security Bypass; Pivoting and Lateral Movement; Privileged Insider Network Attacks; Covering Tracks; Defense Spotlight: Real Intelligence Threat Analytics (RITA); Post-Exploitation Data Collection; Where To Go From Here

SECTION 6: Capture-the-Flag Event

Over the years, the security industry has become smarter and more effective in stopping attackers. Unfortunately, attackers themselves are also getting smarter and more sophisticated. One of the most effective ways to stop an adversary is to actually test the environment with the same tools and tactics that the attacker will use against you. Our Capture-the-Flag event is a full day of hands-on activity that involves you working as a consultant for a fictitious company that has recently been compromised. You will apply all of the skills you've learned in class, using the same techniques attackers use to compromise modern, sophisticated network environments. Working together as teams, small groups will scan, exploit, and complete post-exploitation tasks against a cyber range of target systems including Windows, Linux, Internet of Things, and cloud targets. This hands-on challenge is designed to help players practice their skills and reinforce concepts learned throughout the course while challenging each individual player in an environment that replicates modern networks. Powered by the NetWars engine, the event guides players to successfully compromise target systems, bypass endpoint protection platforms, pivot to internal network high-value hosts, and exfiltrate data that are of greatest value to the target organization. The winners will win the coveted SEC504 challenge coin.

TOPICS: Hands-on Analysis