SEC504: Hacker Tools, Techniques, and Incident Handling

GCIH Incident Handler giac.org/gcih

6 Day Program | 38 CPEs | Laptop Required

You Will Learn

- How to apply a dynamic approach to incident response
- How to identify threats using host, network, and log analysis
- Best practices for effective cloud incident response
- Cyber investigation processes using live analysis, network insight, and memory forensics
- Defense spotlight strategies to protect critical assets
- Attacker techniques to evade endpoint detection tools
- How attackers exploit complex cloud vulnerabilities
- Attacker steps for internal discovery and lateral movement after an initial compromise
- The most effective attacks to bypass system access controls
- The crafty techniques attackers use, and how to stop them

The goal of modern cloud and on-premises systems is to prevent compromise, but the reality is that detection and response are critical. Keeping your organization out of the breach headlines depends on how well incidents are handled to minimize loss to the company.

In SEC504, you will learn how to apply a dynamic approach to incident response. Using indicators of compromise, you will practice the steps to effectively respond to breaches affecting Windows, Linux, and cloud platforms. You will be able to take the skills and hands-on experience gained in the course back to the office and apply them immediately.

Understanding the steps to effectively conduct incident response is only one part of the equation. To fully grasp the actions attackers take against an organization, from initial compromise to internal network pivoting, you also need to understand their tools and techniques. In the hands-on environment provided by SEC504, you ll use the tools of the attackers themselves in order to understand how they are applied and the artifacts the attackers leave behind. By getting into the mindset of attackers, you will learn how they apply their trade against your organization, and you ll be able to use that insight to anticipate their moves and build better defenses.

Author Statement

"Attacker tools and techniques have changed, and we need to change our incident response techniques to match. Since I took over as author of SEC504 in 2019, I have rewritten the entire course to give you the skills you need to succeed at incident response. Whether the attacks are Windows-focused or involve attacking critical database platforms or exploiting cloud vulnerabilities, you'll be prepared to effectively identify the attack, minimize the impact, and respond efficiently. With your knowledge of hacker tools and techniques, and by using defense skills that dramatically improve security, you will be ready to become the subject-matter expert your organization needs to meet today's cyber threats."

—Joshua Wright

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)

"SEC504 is a great class overall that is perfect for pen testers and defenders alike. It has greatly helped me understand how attackers think, how they gather information, and how they maintain and gain control of systems."

—Evan Brunk, **Acuity Insurance**

"Great content! As a developer it is extremely useful to understand exploits and how better coding practices help your security position."

—Alex Colclough, **Clayton Homes**

Section Descriptions

SECTION 1: Incident Response and Cyber Investigations

The first section of SEC504 focuses on how to develop and build an incident response process in your organization by applying the Dynamic Approach to Incident Response (DAIR) to effectively verify, scope, contain, assess, and remediate threats. We'll apply this process in-depth with hands-on labs and examples from real-world compromises.

TOPICS: Incident Response; Digital Investigations; Live Examination; Network Investigations; Memory Investigations; Malware Investigations; Cloud Investigations; Bootcamp: Linux Olympics

SECTION 2: Recon, Scanning, and Enumeration Attacks

In this course section we'll look at the techniques attackers use to conduct reconnaissance as a pre-attack step, including how they use open-source intelligence, network scanning, and target enumeration attacks to find the gaps in your network security. You'll use attacker techniques to assess the security of a target network, evaluating popular protocols and endpoints for Windows, Linux, and cloud targets. After delivering the attacks, you'll investigate the logging data and evidence that remains to recognize these attacks as they happen.

TOPICS: MITRE ATT&CK Framework Introduction; Open-Source Intelligence; DNS Interrogation; Website Reconnaissance; Network and Host Scanning with Nmap; Cloud Spotlight: Cloud Scanning; Enumerating Shadow Cloud Targets; Server Message Block (SMB) Sessions; Defense Spotlight: DeepBlueCLI

SECTION 3: Password and Access Attacks

Password attacks are the most reliable mechanism for attackers to bypass defenses and gain access to your organization's assets. In this course section we'll investigate the complex attacks that exploit password and multi-factor authentication weaknesses using the access gained to access other network targets.

TOPICS: Password Attacks; Understanding Password Hashes; Password Cracking; Defense Spotlight: Domain Password Audit Tool (DPAT); Cloud Spotlight: Insecure Storage; Multi-Purpose Netcat

SECTION 4: Public-Facing and Drive-By Attacks

In this course section we'll begin our look at target exploitation frameworks that take advantage of weaknesses on public servers and client-side vulnerabilities. Using the implicit trust of a public website, you'll apply attacker tools and techniques to exploit browser vulnerabilities, execute code with Microsoft Office documents, and exploit the many vulnerabilities associated with vulnerable web applications.

TOPICS: Metasploit Framework; Drive-By Attacks; Defense Spotlight: System Resource Usage Monitor; Command Injection; Cross-Site Scripting (XSS); SQL Injection; Cloud Spotlight: SSRF and IMDS Attacks

SECTION 5: Evasion and Post-Exploitation Attacks

Building on password, public-facing, and drive-by attacks, we'll look at the attacks that happen after initial exploitation. You'll see how attackers bypass endpoint protection systems and use an initial foothold to gain access to internal network targets. You'll then apply the techniques you learn with privileged insider Local Area Network (LAN) attacks, using privileged access to establish persistence, how attackers scan for and collect data from a compromised organization. You will apply these skills to assess the security risks of a vulnerable cloud deployment through visualization and automated assessment techniques. Finally, we'll look at the steps to take after the course is over, turning what you've learned into long-term skills and helping you prepare for the certification exam.

TOPICS: Endpoint Security Bypass; Pivoting and Lateral Movement; Hijacking Attacks; Covering Tracks; Establishing Persistence; Defense Spotlight: Real Intelligence Threat Analytics; Data Collection; Cloud Spotlight: Cloud Post-Exploitation; Where to Go from Here

SECTION 6: Capture-the-Flag Event

Our Capture-the-Flag event is a full day of hands-on activity that has you working as a consultant for ISS Playlist, a fictitious company that has recently been compromised. You will apply all of the skills you've learned in class, using the same techniques used by attackers to compromise modern, sophisticated network environments. You will work on a team or independently to scan, exploit, and complete post-exploitation tasks against a cyber range of target systems including Windows, Linux, Internet of Things devices, and cloud targets. This hands-on challenge is designed to help players practice their skills and reinforce concepts learned throughout the course. With an integrated hint system to give you the on-demand guidance you need to succeed, the event guides you through the steps to successfully compromise target systems, bypass endpoint protection platforms, pivot to internal network high-value hosts, and exfiltrate company data.

TOPICS: Target Discovery and Enumeration; Applying Open-Source Intelligence and Reconnaissance Information-Gathering; Public-Facing Asset Compromise; Email Compromise; Attacking Windows Active Directory; Password Spray, Guessing, and Credential Stuffing Attacks; Post-Exploitation Pivoting and Lateral Movement; Choosing, Configuring, and Delivering Exploits; Internal Attacker Compromise Attribution

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

"SEC504 has been the single best course I have ever taken. It leaves the student prepared and able to understand a broad scope of content in security."

—Joshua Nielson, **Microsoft**

"Incident response is the most underused aspect in small companies. SEC504 gives us the ability to help management understand the value."

—David Freedman, **Nationwide Payment Solutions**