SEC504: Hacker Tools, Techniques, and Incident Handling

Course Overview

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 handson 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.

Job Roles

- Technical Support Specialist
- Systems Security Analyst
- Privacy Officer/Privacy Compliance Manager
- Cyber Instructional Curriculum Developer
- Cyber Instructor
- Security Awareness & Communications Manager
- Information Systems Security Manager
- Cyber Defense Analyst

Intended Audience

- 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

Duration

6 Days

Certifications

GIAC Certified
Incident Handler (GCIH)

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

SEC504: Hacker Tools, Techniques, and Incident Handling

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Incident Response and Cyber Investigations

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

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

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

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

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

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

Course Objectives

- 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

GIAC Certified Incident Handler (GCIH)

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)