Hacker Techniques, Exploits & Incident Handling (GCIH)

Course Description:

Incident handlers manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on detecting, responding, and resolving computer security incidents and covers the following security techniques:

- The steps of the incident handling process
- Detecting malicious applications and network activity
- Common attack techniques that compromise hosts
- Detecting and analyzing system and network vulnerabilities
- Continuous process improvement by discovering the root causes of incidents

Audience:

*Students must bring their laptops.

For attendances who do not wish to build a dual boot machine. We will give you a DVD full of attack tools to experiment with during the class and take home for later analysis. We will also provide a Linux image with all of our tools pre-installed that runs within VMware Player or VMware Workstation.

Target:

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

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
Certificate Benefits:

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.

- 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

You will be able to:

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques to be able to evaluate an attackers spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, back-doors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attackers presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attackers activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attackers activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access of a target machine using Metasploit, and then detecting the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
• Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
• Employ the netstat and Isosf tools to diagnose specific types of traffic-flooding denial-of-service techniques and choosing appropriate response actions based on each attacker's flood technique
• Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

Course Syllabus:

• SEC504.1: Incident Handling Step-by-Step and Computer Crime Investigation
• SEC504.2: Computer and Network Hacker Exploits - Part 1
• SEC504.3: Computer and Network Hacker Exploits - Part 2
• SEC504.4: Computer and Network Hacker Exploits - Part 3
• SEC504.5: Computer and Network Hacker Exploits - Part 4
• SEC504.6: Hacker Tools Workshop

Course Topics:

The topic areas for each exam part follow:

• **Backdoors & Trojan Horses**
The candidate will demonstrate a detailed understanding of how Backdoors are used to gain access to systems, and how to defend systems.

• **Buffer Overflows**
The candidate will demonstrate an understanding of what a buffer overflow is, how they are created, and how to defend against them. Additionally, candidates will demonstrate a high-level understanding of how attackers use common tools to create and maintain a backdoor on a compromised system.

• **Covering Tracks: Networks**
The candidate will demonstrate an understanding of how attackers use tunneling and covert channels to cover their tracks on a network, and the strategies involved in defending against them.

• **Covering Tracks: Systems**
The candidate will demonstrate an understanding of how attackers hide files and directories on Windows and Linux hosts and how they attempt to cover their tracks.

• **Denial of Service Attacks**
The candidate will demonstrate a comprehensive understanding of the different kinds of Denial of Service attacks and how to defend against them.

• **Exploiting Systems using Netcat**
The candidate will demonstrate an understanding of how to properly use the Netcat utility and how to defend against it.
• **Format String Attacks**
  The candidate will demonstrate a comprehensive understanding of how format string attacks work and how to defend against them.

• **Incident Handling Overview and Preparation**
  The candidate will demonstrate an understanding of what Incident Handling is, why it is important, and an understanding of best practices to take in preparation for an Incident.

• **Incident Handling Phase 2 Identification**
  The candidate will demonstrate an understanding of important strategies to gather events, analyze them, and determine if we have an incident.

• **Incident Handling Phase 3 Containment**
  The candidate will demonstrate an understanding of high-level strategies to prevent an attacker from causing further damage to the victim after discovering the incident.

• **Incident Handling: Recovering and Improving Capabilities**
  The candidate will demonstrate an understanding of the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and "lessons learned" meetings.

• **IP Address Spoofing**
  The candidate will demonstrate an understanding of what IP Spoofing is, the three different types of spoofing, and strategies to defend against it.

• **Network Sniffing**
  The candidate will know what network sniffing is, how to use common sniffing tools, and how to defend against sniffers.

• **Password Attacks**
  The candidate will demonstrate a detailed understanding of the three methods of password cracking.

• **Reconnaissance**
  The candidate will demonstrate an understanding of public and open source reconnaissance techniques.

• **Rootkits**
  The candidate will demonstrate an understanding of how user-mode and kernel-mode rootkits operate, what their capabilities are and how to defend against them.

• **Scanning: Host Discovery**
  The candidate will demonstrate an understanding of the tools and techniques used for host discovery on wired and wireless networks.

• **Scanning: Network and Application Vulnerability scanning and tools**
  The candidate will demonstrate an understanding of the fundamentals of network and application vulnerability scanners, common commercial and open source tools, and how to defend against them.
- Scanning: Network Devices (Firewall rules determination, fragmentation, and IDS/IPS evasion)
The candidate will demonstrate an understanding of how to use Firewalk to determine firewall policies, the general principles of IP fragmentation attacks, why they are used, as well as the ability to identify them.

- Scanning: Service Discovery
The candidate will demonstrate an understanding of the tools and techniques used for network mapping, port scanning, and passive fingerprinting techniques and how to defend against them.

- Session Hijacking, Tools and Defenses
The candidate will demonstrate an understanding of the definition of session hijacking, the two methods commonly used and why it is effective. Additionally, the candidate will demonstrate an understanding of how to identify common hijacking tools and the strategies to prepare for, identify and contain hijacking attacks.

- Types of Incidents
The candidate will demonstrate an understanding of multiple types of incidents, including espionage, unauthorized use, intellectual property, and insider threats and apply strategies to prevent or address these cases.

- Virtual Machine Attacks
The candidate will demonstrate an understanding of the virtual machine environment from an attackers perspective, including targets and detection, and how to defend against threats.

- Web Application Attacks
The candidate will demonstrate an understanding of the value of the Open Web Application Security Project (OWASP), as well as different Web App attacks such as account harvesting, SQL injection, Cross-Site Scripting and other Web Session attacks.

- Worms, Bots & Bot-Nets
The candidate will demonstrate a detailed understanding of what worms, bots and bot-nets are, and how to protect against them.
### Type of Certificate Obtained:
- SEC504: Hacker Techniques, Exploits & Incident Handling

### Format:
- Instructor-Led Training/Classroom

### Course Duration:
- 6 days - Including refreshments, lunch and course notes.

### Total Training Hours:
- 48 hours

### Language:
- English