SEC501: Advanced Security Essentials – Enterprise Defender

GCED Enterprise Defender giac.org/gced

6 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Build a defensible network architecture by auditing router configurations, launching successful attacks against them, hardening devices to withstand those same attacks, and using active defense tools to detect an attack and generate an alert
- Perform detailed analysis of traffic using various sniffers and protocol analyzers, and automate attack detection by creating and testing new rules for detection systems
- Identify and track attacks and anomalies in network packets
- Use various tools to assess systems and web applications for known vulnerabilities, and exploit those vulnerabilities using penetration testing frameworks and toolsets
- Analyze Windows systems during an incident to identify signs of a compromise
- Find, identify, analyze, and clean up malware such as Ransomware using a variety of techniques, including monitoring the malware as it executes and manually reversing its code to discover its secrets

GCED Enterprise Defender giac.org/gced

GIAC Certified Enterprise Defender

The GIAC Certified Enterprise Defender (GCED) certification builds on the security skills measured by the GIAC Security Essentials certification. It assesses more advanced, technical skills that are needed to defend the enterprise environment and protect an organization as a whole. GCED certification holders have validated knowledge and abilities in the areas of defensive network infrastructure, packet analysis, penetration testing, incident handling and malware removal.

- Incident handling and computer crime investigation
- Computer and network hacker exploits
- Hacker tools (Nmap, Nessus, Metasploit and Netcat)

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and appropriately respond to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of where it resides or what paths it travels.

The primary way to PREVENT attacks begins with assuring that your network devices are optimally configured to thwart your adversary. This is done by auditing against established security benchmarks, hardening devices to reduce their attack surface, and validating their increased resilience against attack. Prevention continues with securing hostname resolution (an obvious adversary target for establishing a Machine-in-the-Middle position) and goes even further with securing and defending cloud infrastructure (both public and private) against compromise.

Enterprises need to be able to DETECT attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, monitoring for indications of compromise, and employing active defense techniques to provide early warning of an attack. Of course, despite an enterprise's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Performing penetration testing and vulnerability analysis against your enterprise to identify problems and issues before a compromise occurs is an excellent way to reduce overall organizational risk.

Once an attack is identified, you must quickly and effectively RESPOND, activating your incident response team to collect the forensic artifacts needed to identify the tactics, techniques, and procedures being used by your adversaries. With this information you can contain their activities, ensure that you have scoped out all systems where they have had an impact, and eventually eradicate them from the network. This can be followed by recovery and remediation to PREVENT their return. Lessons learned through understanding how the network was compromised can then be fed back into more preventive and detective measures, completing the security lifecycle.

It costs enterprises worldwide billions of dollars annually to respond to malware, and particularly Ransomware, attacks. So it is increasingly necessary to understand how such software behaves. Ransomware spreads very quickly and is not stealthy; as soon as your data become inaccessible and your systems unstable, it is clear something is amiss. Beyond detection and response, when prevention has failed, understanding the nature of malware, its functional requirements, and how it achieves its goals is critical to being able to rapidly reduce the damage it can cause and the costs of eradicating it.

Business Takeaways

- Improve the effectiveness, efficiency, and success of cybersecurity initiatives
- Build defensible networks that minimize the impact of attacks
- Identify your organization's exposure points to ultimately prioritize and fix the vulnerabilities, increasing the organization's overall security

Section Descriptions

SECTION 1: Defensive Network Architecture

Section 1 will focus on security in the design and configuration of various enterprise infrastructures. From a security perspective, proper design and configuration protects both the components being configured and the rest of the enterprise that depends on that gear to defend other components from attacks. In other words, a good house needs a good foundation! We will discuss published security benchmarks, vendor guidance to secure various products, and regulatory requirements and how they impact defending infrastructure against specific attacks. To illustrate these points, we will look in detail at securing and defending a router infrastructure against a number of device- and network-based attacks. Securing private and public cloud infrastructure against common attacks will also be discussed.

TOPICS: Security Standards and Audit; Authentication, Authorization, and Accounting; Defending Network Infrastructure; Intrusion Prevention Systems and Firewalls; Name Resolution Attacks and Defense; Securing Private and Public Cloud Infrastructure

SECTION 2: Penetration Testing

Security is all about understanding, mitigating, and controlling the risk to an enterprise's critical assets. An enterprise must understand the changing threat landscape and have the capacity to compare it against its own vulnerabilities that could be exploited to compromise the environment. This second course section will present the variety of tests that can be run against an enterprise and show how to perform effective penetration tests to better understand the security posture for network services, operating systems, and applications. In addition, we will talk about social engineering and reconnaissance activities to better emulate increasingly prevalent threats to users. Finding basic vulnerabilities is easy but not necessarily effective if these are not the vulnerabilities attackers exploit to break into a system. Advanced penetration testing involves understanding the variety of systems and applications on a network and how they can be compromised by an attacker. Students will learn about scoping and planning their test projects, performing external and internal network penetration testing and web application testing, and pivoting through the environment like real-world attackers. Penetration testing is critical to identify an enterprise's exposure points, but students will also learn how to prioritize and fix these vulnerabilities to increase the enterprise's overall security.

TOPICS: Penetration Testing Scoping and Rules of Engagement; Online Reconnaissance; Social Engineering; Network Mapping and Scanning Techniques; Enterprise Vulnerability Scanning; Network Exploitation Tools and Techniques; Post-Exploitation and Pivoting; Web Application Exploitation Tools and Techniques; Reporting and Debriefing

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

SECTION 3: Security Operations Foundations

Traffic analysis and intrusion detection used to be treated as a separate discipline within many enterprises. Today, prevention, detection, and response must be closely knit, so that once an attack is detected, defensive measures can be adapted and proactive forensics implemented so the enterprise can continue to operate. This course section will start with a brief introduction to network security monitoring, followed by a refresher on network protocols with an emphasis on fields to look for as security professionals. We will use tools such as tcpdump and Wireshark to analyze packet traces and look for indicators of attacks. We will use a variety of detection and analysis tools, craft packets with Scapy to test detection, and touch on network forensics and the Security Onion monitoring distribution. Students will also explore Snort as a Network Intrusion Detection System and examine rule signatures in-depth.

TOPICS: Network Security Monitoring; Advanced Packet Analysis; Network Intrusion Detection/Prevention; Writing Signatures for Detection; Network Forensics and More; Event Management Introduction; Continuous Monitoring; Logging and Event Collection and Analysis; SIEM and Analytics

SECTION 4: Digital Forensics and Incident Response

This section begins with a discussion of Active Defense approaches in some detail. Next, we will present the core concepts of both Digital Forensics and Incident Response. We will explore some of the hundreds of artifacts that can give forensic investigators specific insight about what occurred during an incident. Students will learn how incident response currently operates, after years of evolving, in order to address the dynamic procedures used by attackers to conduct their operations. We will also look at how to integrate DFIR practices into a continuous security operations program. The section will cover the general guidelines for a cyclical, six-step incident response process. Each step will be examined in detail, including practical examples of how to apply it. Finally, students will learn about the artifacts that can best be used to determine the extent of suspicious activity within a given environment and how to migrate techniques to a large data set for enterprise-level analysis.

TOPICS: Active Defense; DFIR Core Concepts: Digital Forensics; DFIR Core Concepts: Incident Response; Modern DFIR; Widening the Net: Scaling & Scoping

SECTION 5: Malware Analysis

Malicious software is responsible for many incidents in almost every type of organization. Types of malware vary widely, from Ransomware and Rootkits to Crypto Currency Miners and worms. We will define each of the most popular types of malware and walk through multiple examples. The four primary phases of malware analysis will be covered: Fully Automated Analysis, Static Properties Analysis, Interactive Behavior Analysis, and Manual Code Reversing. You will complete various in-depth labs requiring you to fully dissect a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tricking the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.

TOPICS: Introduction to Malware Analysis; Malware Analysis Stages: Fully Automated and Static Properties Analysis; Malware Analysis Stages: Interactive Behavior Analysis; Malware Analysis Stages: Manual Code Reversing

SECTION 6: Enterprise Defender Capstone

The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use the skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they submit flags to score points. More difficult challenges will be worth more points. In this defensive exercise, challenges include packet analysis, routing protocols, scanning, malware analysis, and other challenges related to the course material.

"If you want to take a deep-dive into enterprise security, then you must take SEC501."

— Nikolai Vinogradov, **JSC Severstal Management**