SEC460

Enterprise Threat and Vulnerability Assessment

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Vulnerability assessors
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- System administrators

You Will Be Able To

- Perform end-to-end vulnerability assessments
- Develop customized vulnerability discovery, management, and remediation plans
- Conduct threat intelligence gathering and analysis to create a tailored cybersecurity plan that integrates various attack and vulnerability modeling frameworks
- Implement a proven testing methodology using industry-leading tactics and techniques
- Adapt information security approaches to target real-world enterprise challenges
- Configure and manage vulnerability assessment tools to limit risk added to the environment by the tester
- Operate enumeration tools like Nmap, Kansa, Bloodhound, and WPScan to identify network nodes, services, configurations, and vulnerabilities that an attacker could use as an opportunity for exploitation
- Conduct infrastructure vulnerability enumeration at scale across numerous network segments, in spite of divergent network infrastructure and nonstandard configurations
- Conduct web application vulnerability enumeration in enterprise environments while solving complex challenges resulting from scale
- Perform manual discovery and validation of cybersecurity vulnerabilities that can be extended to custom and unique applications and systems
- Manage large vulnerability datasets and perform risk calculation and scoring against organization-specific risks
- Implement vulnerability triage and prioritize mitigation
- Interact with and operate on complex network environments, while accounting for infrastructure obstacles like DLP solutions, IDS/IPS, Proxies, Nextgen Firewalls, and layer-7 filtering devices
- Craft custom PowerShell scripts to enhance your operations, gain increased insight, scale mitigation tactics, and outsource skills to less skilled team members

Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. **SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise.** The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools, and a proven testing methodology.

This course takes you beyond the checklist, giving you a tour of the attackers' perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. **By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your medium- or large-scale organization.**

SANS

www.sans.org/SEC460

460.1 Methodology, Planning, and Threat Modeling

In this section of the course, students will develop the skills needed to conduct high-value vulnerability assessments with measurable impact. We will explore the elemental components of successful vulnerability assessment programs, deconstruct the logistical precursors to value-added operations, and integrate adversarial threat modeling and intelligence. Scale and architecture are major challenges to an enterprise. We will discuss techniques and strategies to overcome these obstacles, and perform a table-top exercise to connect theory with reality. We will also dive into fundamental information security topics, explore the nuanced differences between major categories of services, and examine the industry's foremost methodologies for vulnerability assessment. We will examine the strategic influences that impact a typical enterprise and its vulnerability management program.

Topics: **Maximizing Value from Vulnerability Assessments and Programs; Setting Up for Success at Scale: Enterprise Architecture and Strategy; Developing Transformational Vulnerability Assessment Strategies; Performing enterprise threat modelling; Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload; The Vulnerability Assessment Framework; Overview of Comprehensive Network Scanning; Compliance Standards and Information Security**

460.2 Discovery

Having mastered the structural foundations of vulnerability management, we pivot to the realm of direct, tactical application. Comprehensive reconnaissance, enumeration, and discovery techniques are the prime elements of successful vulnerability assessment. While gaining additional familiarity with hands-on enterprise operations, you will systematically probe the environment in order to discover the relevant host, service, version, and configuration details that will drive the remainder of the assessment system. As we begin active scrutiny of the enterprise, you will learn how to interpret tool output and form a detailed network map. We will explore proven methods to ensure the integrity of our dataset as we identify IP addresses, operating systems, platforms, and services. The day culminates with an introduction to the PowerShell scripting language focusing on large-scale system management, vulnerability discovery, and mitigation.

Topics: **Active and Passive Reconnaissance; Identification and Enumeration with DNS; DNS Zone Speculation and Dictionary-Enabled Discovery; Port Scanning with Nmap and Zenmap; Scanning Large-Scale Environments; Commonplace Services; Scanning the Network Perimeter and Engaging the DMZ; The Windows Domain: Exchange, SharePoint, and Active Directory; Recruiting Disparate Data Sources: Patches, Hotfixes, and Configurations; Trade-offs: Speed, Efficiency, Accuracy, and Thoroughness; Introduction to PowerShell**

460.3 Enhanced Vulnerability Scanning and Automation

We begin day three by delving into the next phase of the Vulnerability Assessment Framework and charging into the most exciting topic in security testing: automation to handle scale. We start by breaking vulnerability scanning into its elemental components and gaining an understanding of vulnerability measurement that can be applied to task automation. This focus will direct us to the quantitative facets underlying cybersecurity vulnerabilities and drive our discussion of impact, risk, and triage. Each topic discussed will focus on identifying, observing, inciting, or assessing the entry points that threats leverage during network attacks. Later in the day, we will apply our understanding of the vulnerability concept to evolve our PowerShell skills and take action on an enterprise scale. This portion of the course is dedicated to learning by application and translates easily to frontline operations. We'll use premier industry tools like Rapid7's Nexpose, while simultaneously exploring manual testing procedures. We'll also cover application-specific testing tools and techniques to provide you with a broad perspective and actionable experience.

Topics: **Enhanced Vulnerability Scanning; Risk Assessment Matrices and Rating Systems; Quantitative Analysis Techniques Applied to Vulnerability Scoring; Performing Tailored Risk Calculation to Drive Triage; General Purpose vs. Application Specific Vulnerability Scanning; Tuning the Scanner to the Task, the Enterprise, and Tremendous Scale; Scan Policies and Compliance Auditing; Performing Vulnerability Discovery with Open-Source and Commercial Appliances; Nmap Scripting Engine and OpenVAS; Testing for Insecure Cryptographic Implementations Including SSL; Assessing VOIP Environments; Discovering Vulnerabilities in the Enterprise Backbone: Active Directory, Exchange, and SharePoint; Evaluating Vulnerability Risk in Custom and Unique Systems including Web Applications; Minimizing Supplemental Risk while Conducting Authenticated Scanning through Purposeful Application of Least Privilege; Probing for Data Link Liability to Identify Hazards in Wireless Infrastructure, Switches, and VLANs; Manual Vulnerability Discovery Automated to Attain Maximal Efficacy**

460.4 Vulnerability Validation, Triage, and Data Management

Over the course of this day we will tackle the next phase of our overarching testing methodology, vulnerability validation, while simultaneously confronting the biggest headaches common to a vulnerability assessment at scale. At large scale, vulnerability data can be overwhelming and possibly even contradictory. We will cover the specific techniques needed to wade through and better focus those data. Next, we will examine techniques for collaboration and data management with the Acheron tool for analyzing vulnerability data across an organization.

Topics: **Assigning a Confidence Value and Validating Exploitative Potential of Vulnerabilities; Manual Vulnerability Validation Targeting Enterprise Infrastructure; Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base; Managing Large Repositories of Vulnerability Data; Querying the Vulnerability Knowledge Base; Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk**

460.5 Remediation and Reporting

Many well-intentioned vulnerability assessment programs begin with zeal and vitality, but after the discovery of vulnerabilities there is often a tendency to ignore the risk reality and shift back to the status quo. Over the previous course modules we focused on knowing the target environment and uncovering its weak points. Now it's time for decision and action based on an understanding of the risks the organization faces. Developing an actionable vulnerability remediation plan with time-based success targets sets the stage for continuous improvement, and that's exactly what we cover in this section of the course. Developing this plan in conjunction with the Vulnerability Assessment Report is an opportunity to galvanize the team, while enhancing the vulnerability assessment value proposition.

Topics: **Team Operations and Collaboration; Security Operations Project Management Essentials; Transforming Triage Listing into the Vulnerability Remediation Plan; Developing the Cybersecurity Risk Sight Picture; Connecting Related Datasets and Framing the Narrative; Developing a Web of Network and Host Affiliations; Modeling Account Relationships on Active Directory Forests; Creating Effective Vulnerability Assessment Reports; Curbing the Vulnerability Lifecycle and Aspiring to Zero Hour; Closure: Be a Positive Influence in the Context of the Global Information Security Crisis**

460.6 Vulnerability Assessment Foundry

In celebration of your diligence, curiosity, and mad new vulnerability skills, we welcome you to your final hands-on challenge to hammer home your capabilities. The guided scenario on this final course day is designed to test your mettle through trial and detailed work in a fun capture-the-flag-style environment. The challenge is the canvas upon which you can hone your skills and measure your maturing talents. Armed for the fight, you will doubtless rise to the challenge... and triumph! The scenario: An organization called "The Foundry" has engaged you to perform a vulnerability assessment of its environment. The organization is very aware of your particular set of vulnerability assessment skills, and treasures the insights it is certain you will provide to help secure the organization against its formidable adversaries, including nefarious cybercrime cartels and jealous nation-state actors. Teams will work together to help squash issues that would lead to a compromise of The Foundry's precious assets.

Topics: **Tactical Employment of the Vulnerability Assessment Framework; Threat Modeling; Discovery; Vulnerability Scanning; Validation; Data Management and Triage**

SANS

SEC460 Training Formats

(subject to change)

Live Training

www.sans.org/security-training/by-location/all

"It cannot be stated enough that SANS provides an INCREDIBLE amount of training for what you pay. No one else compares."

-Ron Foupht, Sirius Computer Solutions