AUD507: Auditing Networks, Perimeters, and Systems

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

www.giac.org

www.sans.edu


DoD 8570 Required
www.sans.org/8570

Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper network risk assessment to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks—a standard to conduct an audit against
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- Audit web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

"By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. I cannot imagine another class that forces you to use real tools in real situations. It is just like gaining real world experience."

-Jay Russell, U.S. Navy

507.1 Effective Auditing, Risk Assessment, Reporting & Cloud Computing

After laying the foundation for the role and function of an auditor in the information security field, this day's material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and helping you recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions when dealing with virtualization and with Cloud Computing.

Topics: Auditor's Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

507.2 HANDS ON: Auditing the Perimeter

Focus on some of the most sensitive and important parts of our information technology infrastructure: routers and firewalls. In order to properly audit a firewall or router, we need to clearly understand the total information flow that is expected for the device. Diagrams will allow the auditor to identify what objectives the routers and firewalls are seeking to meet, thus allowing controls to be implemented that can be audited. Overall, this course will teach the student everything needed to audit routers, switches, and firewalls in the real world.

Topics: Overview; Detailed Audit of a Router; Auditing Switches; Testing the Firewall; Testing the Firewall Rulebase; Testing Third-Party Software; Reviewing Logs and Alerts; The Tools Used

507.3 HANDS ON: Web Application Auditing

Web Applications have consistently been rated as one of the top five vulnerabilities that enterprises face for the past several years. Unlike the other top vulnerabilities, however, our businesses continue to accept this risk since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough.

Topics: Identify Controls Against Information Gathering Attacks; Process Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-On Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web-Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-Side Techniques for Protecting Your Customers and Their Sensitive Data

AUD507 Training Formats

(subject to change)

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

Community SANS
www.sans.org/community

Mentor Program
www.sans.org/mentor

OnSite
www.sans.org/onsite

vLive
www.sans.org/vlive

OnDemand
www.sans.org/ondemand

SelStudy
www.sans.org/selfstudy

507.4 HANDS ON: Advanced Windows Auditing

Microsoft's business class system makes up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This class gives you the keys, techniques and tools to build an effective long-term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

Topics: Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

507.5 HANDS ON: Auditing Unix Systems

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as, access controls and security models.

Topics: Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

507.6 HANDS ON: Audit the Flag: A NetWars Experience

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well-known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

Topics: Technologies Included in the Capstone Challenges: Network Devices, Servers, Applications, and Workstations