AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

GSNA
Systems and Network Auditor
giac.org/gsna

6 Day Program | 36 CPEs | Laptop Required

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 risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
- Establish a well-secured baseline for computers and networks as a standard to conduct audit against
- Perform a network and perimeter audit using a repeatable process
- Audit virtualization hosts and container environments to ensure properly deployment and configuration
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system which will baseline and automatically audit Active Directory and all systems in a Windows domain
- Utilize scripting to build a system which will baseline and automatically audit Linux systems

Performing IT security audits at the enterprise level can be a daunting task. How should you determine which systems to audit first? How do you assess the risk to the organization related to information systems and business processes? What settings should you check 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? How do you turn this into a continuous monitoring process? The material covered in this course will answer all of these questions and more.

AUD507 teaches students how to apply risk-based decision making to the task of auditing enterprise security.

This track 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, students will have the opportunity to delve into the technical "how-to" for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

AUD507 allows students to practice new skills in realistic, hands-on labs.

In this course, students learn how to use technical tests to develop the evidence needed to support their findings and recommendations. Each day affords students opportunities to use the tools and techniques discussed in class, with labs designed to simulate real-world enterprise auditing challenges and to allow the students to use appropriate tools and techniques to solve these problems.

We also go beyond simply discussing the tools students could use; we give them the experience to use the tools and techniques effectively to measure and report on the risk in their organizations. The final section of the course is a lab that lets students challenge themselves by solving realistic audit problems using and refining what they have learned in class.

The skills students learn in AUD507 can be used immediately after class.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

> **"AUD507 provides insight on different aspects related to system configurations and associated risks."**
>
> — Yosra Al-Basha, **Yemen LNG Co.**

Section Descriptions

SECTION 1: Enterprise Audit Fundamentals; Discovery and Scanning Tools

Section one provides the "on-ramp" for the highly technical audit tools and techniques used later in the week. After laying the foundation for the role and function of an auditor in the information security field, this day's material provides practical, repeatable and useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and enabling us to recommend additional controls to address the risk. We finish off the day with coverage of the security risks and associated audit techniques for virtualization hosts, cloud services and container systems.

TOPICS: Auditor's Role as it Relates to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Network Population Monitoring: Vulnerability Scanning

SECTION 2: Auditing Private and Public Clouds, Containers, and Networks

Section two focuses on securing the enterprise network. The days are gone when a good firewall at the edge of the network is all we really need. In fact, in many enterprises, the network has no real "edge." Auditors should encourage their organizations to focus on security within the network with the same diligence as they use at the perimeter.

TOPICS: Public, Private and Hybrid Cloud Deployments; Private Clouds and Hypervisor Security; Public Cloud Technologies; Shared Responsibility Models; Containers, Orchestration and Serverless Functions; Secure Layer 2 Configurations; Router & Switch Configuration Security; Firewall Auditing, Validation & Monitoring; Wireless

SECTION 3: Web Application Auditing

Web applications seem to stay at the top of the list of security challenges faced by enterprises today. The organization needs an engaging and cutting-edge web presence, but the very technologies which allow the creation of compelling and data-rich websites also make it very challenging to provide proper security for the enterprise and its customers. Unlike other enterprise systems, our web applications are freely shared with the world and exposed to the potential for constant attack.

TOPICS: Why Web Applications Are a Major Problem; Understanding HTTP, HTML, and Related Technologies; Related Technologies; The Burp Proxy; OWASP Top 10 List; OWASP Top 10 Proactive Controls; Server Configuration; Secure Development Practices; Authentication; Session Handling; Data Handling; Logging and Monitoring

SECTION 4: Advanced Windows Auditing and Monitoring

The majority of systems encountered on most enterprise audits are running Microsoft Windows in some version or another. The centralized management available to administrators has made Windows a popular enterprise operating system. The sheer volume of settings and configurable controls, coupled with the large number of systems often in use, makes auditing Windows servers and workstations a huge undertaking. During section four, we teach students how to audit Windows systems and Active Directory domains at scale.

TOPICS: Windows Support and End of Life; PowerShell Command Essentials; PowerShell Scripting; Windows Management Instrumentation (WMI); PowerShell, DSQuery and LDAP; Password Management and Auditing; User Right Assignments; System Security Settings; File and Share Permissions; Registry Permissions and Settings; Windows Logging; Continuous Monitoring for Windows

SECTION 5: Advanced UNIX Auditing and Monitoring

While many enterprises today use Microsoft Windows for their endpoint systems, Linux and other Unix variants are well-established as servers, security appliances and in many other roles. Given the nature of the work these Unix variants do, it is critical to ensure their security. Add to that the fact that mass centralized administration is less likely to occur with these systems, and auditing at scale becomes even more important. Section five uses Debian and CentOS Linux as the example operating systems.

TOPICS: Accreditation and Snowflakes; Linux Basics; Command Line Tools and Scripting; Scripting; System Information; File Permissions; File Integrity; Services; Patching; Users, Groups and Privilege Management; Logging and Monitoring; System Audit Tools; Continuous Monitoring

SECTION 6: Audit the Flag Capstone Exercise

Section six is a capstone exercise which allows students to test and refine the skills learned throughout the course. Using an online "capture the flag" (CTF) engine, students are challenged to audit a simulated enterprise environment by answering a series of questions about the enterprise network, working through various technologies explored during the course. At the conclusion of this section, students are asked to identify the most serious findings within the enterprise environment and to suggest possible root causes and potential mitigations.

TOPICS: Technologies included in the capstone exercise include Network Devices, Servers, Applications, and Workstations

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 auditors 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
- Anyone looking to implement effective continuous monitoring processes within the enterprise

> **"The course is excellent as it covers most of the technical auditing techniques and tools used for auditing."**
>
> — Saeed, **ADNOC-Dist**

GSNA
Systems and Network Auditor
giac.org/gsna

GIAC Systems and Network Auditor

The GIAC Systems and Network Auditor (GSNA) certification validates a practitioner's ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems. GSNA certification holders have demonstrated knowledge of network, perimeter, and application auditing as well as risk assessment and reporting.

- Auditing, risk assessments, and reporting
- Network and perimeter auditing and monitoring, web application auditing
- Auditing and monitoring in windows and Unix environments