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? How do we turn this into a continuous monitoring process? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized 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 are taken 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 controls address. 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 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 help you produce your own checklist, or provide you 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 six 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.

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 gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

You Will Be Able To
• Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
• Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize what will be audited
• Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
• 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 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

“AUD507 provides insight on different aspects related to system configurations and associated risks.”
— Yosra Al-Basha, Yemen LNG Co.
Section Descriptions

SECTION 1: Effective Audit Management, Risk Assessment, and Virtualization Auditing
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; Virtualization & Cloud Computing

SECTION 2: Effective Network and Perimeter Auditing/Monitoring
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: Capturing and Analyzing Network Traffic; Analyzing and Validating Device Configurations; Testing Public Services; Network Mapping and Continuous Monitoring

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 full-day capstone exercise which allows students to test and refine the skills learned throughout the week. 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 the 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