

Automating Technical Auditing

COURSE DURATION: 3-days

CPE HOURS: 24

LEVEL: Intermediate / Group-Live

PREREQUISITES: None

ADVANCE PREPARATION: None

Many Canaudit clients are surprised and impressed with the speed, depth, and professionalism of our audits. Our secret is in the use of specific tools and techniques that enable an auditor to quickly identify and quantify risk. In this workshop, we share our tools and techniques with audit and security professionals. Participants will learn to use a bevy of safe and sane tools that can be used to automate the documentation of the environment and the auditing of specific technologies. In this hands-on workshop, we will focus on audits of the network, the Windows environment, the UNIX and LINUX environment, the Internet, and web applications. The participants in this session will learn how to load and use the software tools in our portable lab. They will learn to identify and eliminate the false positives that often cloud remediation efforts. They will also learn how to present the technical information in exit interviews in a manner that can be easily understood. Report presentation and automating post-audit follow-up are also included.

WHO SHOULD ATTEND

This workshop is intended for IT Auditors and security professionals with at least two years experience. They should have an understanding of network and operating system auditing. There are no prerequisites.

NOTE: Each participant will require a laptop computer with local administrative access rights.

SEMINAR OUTLINE

I INTRODUCTION

- Where do you start?
 - Cataloging the Technical IT Audit Universe
 - Identifying servers by operating system
 - Identifying workstations by operating system
 - Identifying databases in use
 - Preparing the initial Technology Risk Assessment
- Using tools to identify devices (servers, workstations, etc.)
- Using tools to quantify risk within technology group
- Updating the IT Technology Risk Assessment
- Developing the Technology Audit Plan
- Preparing Time and Labor Budgets
- Use of skilled contractors to mitigate staffing limitations

II AUDITING THE NETWORK

- Identifying preliminary network addresses
- Scanning the known network
- Using community strings to glean additional information
- Mapping of network devices, network segments, etc.
- Testing device security
- Determining the use of encryption

- Using checklists to identify additional controls
- Closing meeting (exit interview) techniques
- Writing the audit report
- Automated post-audit follow-up

III AUDITING WINDOWS SERVERS AND WORKSTATIONS

- Scoping the audit
- Identification of security and audit policies
- Determination of specific risk by server and desktop
- Automating patch level management
- Elimination of false positives
- Password analysis
 - Defaults
 - Service accounts
 - Password effectiveness
- Using checklists to identify additional risks
- Compiling the specific risks
- Closing meeting techniques
- Writing the report
- Automated post-audit follow-up

IV AUTOMATING DATABASE SECURITY

- Determination of the RDBMS's in use
- Automating database discovery
- Testing Oracle databases

V

AUDITING INTERNET CONNECTIVITY, WEB SERVERS, AND WEB APPLICATIONS

- Testing MSSQL databases
- Use and review of audit scripts
- Compiling specific risks
- Closing meeting techniques
- Writing the audit report
- Automated post-audit follow-up
- Identifying the official Internet presence
- Determination of the actual Internet presence
- Testing the firewall and Internet-facing network devices
- Testing security appliances
- Testing web servers
- Evaluation in computer Incident Response Procedures
- Testing of web applications
- Elimination of false positives
- Writing the audit report
- Post-audit follow-up

VI

WRAP-UP

- Implementing new techniques
- Roadblocks
- Success indicators
- Developing initial baselines
- Measuring improvement
- Concluding comments