CIW Security Professional Series – Course 3:
Security Auditing, Attacks, and Threat Analysis (November 2002)

Security Auditing, Attacks, and Threat Analysis teaches you how to conduct a security audit. It teaches you how to perform the different phases of an audit, including discovery and penetration. You will also learn how to prevent hackers from controlling your network, and how to generate effective audit reports that can help organizations improve their security and become current with industry security standards. Finally, you will learn about how to recommend industry-standard security solutions for your enterprise. As you examine different threats and learn more about how network hosts participate on a network, you will determine how to assess and manage the risk posed to each system. This course introduces various tools to help you in the auditing process; you will use some of these tools in the labs. You will also study international standards, along with time-tested methods for auditing a network efficiently. After completing this course, you will have in-depth training and experience in analyzing the hacker process and associated methodologies. You will be able to counteract attacks using specific, practical tools, including enterprise-grade security-scanning and intrusion-detection programs. You will also learn how to analyze your findings and make recommendations for establishing the best security possible in a given scenario.

Topics

Security Auditing
Introduction to Auditing
What Is an Auditor?
What Does an Auditor Do?
Auditor Roles and Perspectives
Conducting a Risk Assessment
Risk Assessment Stages

Discovery Methods
Discovery
Security Scans
Enterprise-grade Auditing Applications
Social Engineering
What Information Can You Obtain?

Auditing Server Penetration and Attack Techniques
Network Penetration
Attack Signatures and Auditing
Compromising Services
Common Targets
Routers
Databases
Web and FTP Servers
E-mail Servers
Naming Services
Auditing for System Bugs
Auditing Trap Doors and Root Kits
Auditing Denial-Of-Service Attacks
Combining Attack Strategies
Denial of Service and the TCP/IP Stack

Security Auditing and the Control Phase
Network Control
Control Phase Goals
UNIX Password File Locations
Control Methods
Auditing and the Control Phase

Intrusion Detection
What Is Intrusion Detection?
IDS Applications and Auditing
Intrusion Detection Architecture
IDS Rules
IDS Actions
False Positives
Intrusion-Detection Software
Purchasing an IDS
Auditing with an IDS

Auditing and Log Analysis
Log Analysis
Baseline Creation
Firewall and Router Logs
Operating System Logs
Filtering Logs
Suspicious Activity
Additional Logs
Log Storage
Auditing and Performance Degradation

Audit Results
Auditing Recommendations
Creating the Audit Report
Improving Compliance
Improving Router Security
Enabling Proactive Detection
Host Auditing Solutions
Replacing and Updating Services
Secure Shell (SSH)
SSH and DNS

Target Audience

Network server administrators, firewall administrators, systems administrators, application developers, and IT security officers.

Job Responsibilities

Implement e-business solutions security policies; identify security threats and develop countermeasures using firewall systems and attack-recognition technologies; and manage the deployment of security solutions.

Prerequisites

Students must have completed *Network Security and Firewalls* or be able to demonstrate equivalent Internet knowledge.

Duration

12 hours