POLAR BEAR
CORPORATE EDUCATION SOLUTIONS

SECURITY AUDITING, ATTACKS AND THREAT ANALYSIS

2-days – Course No.PS616

Who Should Attend?

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

Prerequisites:

Students must have passed the CIW Foundations, CIW Server Administrator, and CIW Internetworking Professional exams, and have completed the Network Security and Firewalls and Operating Systems Security courses or have equivalent skills.

Performance Objectives:

Security Auditing, Attacks, and Threat Analysis is a two-day course that teaches students how to perform different phases of a security audit, including discovery and penetration, and how to defeat unauthorized users from controlling company networks. The course discusses how to use Windows NT and Linux to identify security issues and suggest industry-standard solutions. Students will also learn how to generate effective audit reports that can help organizations improve their security and become current with industry security standards.

Course Outline:

Lesson 1: Security Auditing

- Why?
- What Is an Auditor?
- What Does an Auditor Do?
- Auditor Roles and Perspectives
- Conducting a Risk Assessment
- Risk Assessment Stages
- Lesson 1 Assessment Questions

Lesson 2: Discovery Methods

- Discovery
- Security Scans
- Enterprise-grade Auditing Applications
- Scan Levels
- Social Engineering
- What Information Can You Obtain?
- Lesson 2 Assessment Questions

SECURITY AUDITING, ATTACKS AND THREAT ANALYSIS

2-days – Course No.PS616

Lesson 3: Auditing Server Penetration and Attack Techniques

- Network Penetration
- Attack Signatures and Auditing
- Common Targets
- Routers
- Databases
- Web and FTP Servers
- E-mail Servers
- Name Services
- Auditing for System Bugs
- Auditing Trap Doors and Root Kits
- Auditing Denial-Of-Service Attacks
- Buffer Overflow
- Combining Attack Strategies
- The TCP/IP Stack
- Lesson 3 Assessment Questions

Lesson 4: Security Auditing and the Control Phase

- Network Control
- Control Phases
- UNIX Password File Locations
- Control Methods
- Auditing and the Control Phase
- Lesson 4 Assessment Questions

Lesson 5: Intrusion Detection

- Intrusion-Detection Systems
- What Is Intrusion Detection?
- Intrusion-Detection Architecture
- IDS Rules
- False Positives
- Intrusion-Detection Software
- Intruder Alert
- Purchasing an IDS
- Auditing with an IDS
- Lesson 5 Assessment Questions

SECURITY AUDITING, ATTACKS AND THREAT ANALYSIS

2-days – Course No.PS616

Lesson 6: 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
- Lesson 6 Assessment Questions

Lesson 7: Audit Results

- Auditing Recommendations
- Creating the Assessment Report
- Improving Compliance
- Security Auditing and Security Standards
- Improving Router Security
- Enabling Proactive Detection
- Host Auditing Solutions
- Replacing and Updating Services
- Secure Shell (SSH)
- SSH and DNS
- Lesson 7 Assessment Questions

Appendix A: Objectives and Locations

Appendix B: Sample Security Audit Report

Appendix C: Sample Enterprise Scanner Reports

Appendix D: Security Auditing Programs

Appendix E: Installing the TCP/IP Stack Update

Appendix F: Security and Auditing Texts

SECURITY AUDITING, ATTACKS AND THREAT ANALYSIS

2-days – Course No.PS616

Appendix G: Standards Documents

Appendix H: Commercial Products Used in

This Course

- NetRecon and Intruder Alert
- ISS Internet Scanner
- eTrust Intrusion Detection

Appendix I: Internet Security Resources

- General
- UNIX
- Windows NT

Appendix J: Exercise Answers

Appendix K: Works Consulted

Appendix L: Assessment Questions and Answers

Appendix M: Glossary

Appendix N: Supplemental Disk Contents