IS413T
Auditing E-Commerce Systems and IT Infrastructure
[Onsite]

Course Description:

This course offers instruction on security auditing and teaches how to audit a network infrastructure and Web-based applications.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS314T Security Architecture of Common IT Platforms or equivalent

Credit hours: 4

Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

SYLLABUS: Auditing E-Commerce Systems and IT Infrastructure

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

1. Purposes of internal security self-audit
2. Relationship of internal security self-audit to other types of audits
3. Security personnel and their roles
    - Auditing process
    - E-commerce audit policies and regulations
4. E-commerce audit policies and regulations
5. Auditing process
6. Auditable events and collectable data
7. Operating system audits
8. Network infrastructure audits
9. E-commerce application audits
10. Database audits
11. Audit of the audit collection system
12. Automated audit tools

COURSE OBJECTIVES

After successful completion of this course, the students will have the opportunity to:

1. Describe the purpose of the internal security self-audit.
2. Explain the advantages and disadvantages of auditing.
3. Explain the process of auditing e-commerce systems.
4. Identify appropriate guidance for auditing e-commerce systems.
5. Explain the tradeoffs between audit needs and system performance.
6. Conduct an audit of a Windows XP or Windows 2003 system.
7. Conduct an audit of a Linux system.
8. Conduct an audit of a network infrastructure.
9. Describe an audit of an e-commerce application server.
10. Describe an audit of an e-commerce Web interface.
11. Conduct an audit of an e-commerce database.
12. Explain an audit of an audit collection system.
13. List the advantages and disadvantages of automated audit tools.

Related SCANS Objectives

- Acquires security related data and evaluates it for the purpose of auditing E-Commerce and IT infrastructure.
- Classifies security data in an orderly manner so that it can be processed further according to the specific requirements of the organization
- Interprets auditing and effectively communicates the related information.
- Processes auditing information using computers.
- Solves auditing issues as a member of the team.
- Knows how technological systems work and operates effectively within the provided infrastructure.
- Demonstrates competence in monitoring and correcting performance while auditing.
- Demonstrates competence in improving or designing systems while auditing.

- Selects the most suitable technology and methods to determine security needs of the organization.
- Demonstrates how components of a network interact within and outside the network, applying technical skills.
- Troubleshoots the problems related to the activities involved in the process of auditing IT infrastructure for an organization.

TEACHING STRATEGIES

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and delivery tools in the classroom.

COURSE RESOURCES

Student Textbook Package

- Bejtlich, Richard, *The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison Wesley Professional, 2005.*
- INFOSEC Shorts, U.S. Dept. of Defense Information Assurance Training Products
- Planning a Network Infrastructure LabSim DVD and lab manual
- Administering Windows XP Professional LabSim DVD and lab manual

References and Resources

ITT Tech Virtual Library

Log in to the ITT Tech Virtual Library (http://www.library.itt-tech.edu/) to access online books, journals, and other reference resources selected to support ITT Tech curricula.

- General References

>School of Study>School of Information Technology>Professional Organizations>Computer Security Institute

>School of Study>School of Information Technology>Professional Organizations>Information Systems Security Association (ISSA)

>School of Study>School of Information Technology>Recommended Links>IS413 course links>SANS InfoSec Reading Room

- Books

The following books are related to this course and available through the ITT Tech Virtual Library (CRCNetBase):

  - Information Technology Control and Audit, 2nd Edition, Gonzales et al.

- Periodicals

  - Periodicals>EbscoHost

All links to Web references outside of the ITT Tech Virtual Library are always subject to change without prior notice.

EVALUATION & GRADING

COURSE REQUIREMENTS

1. **Attendance and Participation**

   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**

   Each student is responsible for completing all assignments on time.

3. **Team Participation (if applicable)**

   Each student is responsible for participating in team assignments and for completing the delegated task. Each team member must honestly evaluate the contributions by all members of their respective teams.

Evaluation Criteria Table

The final grade will be based on the following weighted categories:

Categories Onsite	Weights (%)
Participation	10%
Lab Assignments	20%
Research Assignments	10%
Case Assignments	10%
Project 1- Part A	5%
Project 1- Part B	5%

Project 2	10%
Project 3	10 %
Final Exam	20%
Total	**100%**

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90 - 100%	4.0
B+	85 - 89%	3.5
B	80 - 84%	3.0
C+	75 - 79%	2.5
C	70 - 74%	2.0
D+	65 - 69%	1.5
D	60 - 64%	1.0
F	<60%	0.0

COURSE OUTLINE

Unit #	Activities for the Unit
1	• **Read** ○ **Chapters 3, 4 and 18:** Gallegos, Frederick, Sandra Senft, Daniel P. Manson, Carol Gonzales. "An Introduction to Computer Security: The NIST Handbook." http://csrc.nist.gov/publications/nistpubs/800-

	12/handbook.pdf • **In-class Discussion 1** • **Lab 1**
2	• **Read** o ITT Tech Virtual Library> Books>CRCNetBase> Book: Information Technology Control and Audit, 2nd Edition>Chapter: Audit and Review: Its Role in Information Technology o Kapp, Justin. "How to Conduct a Security Audit," PC Network Advisor, July 2000. http://www.techsupportalert.com/pdf/t04123.pdf • **Research Assignment 1** • **Case Assignment 1** • **Lab 1** • **In-class Discussion 1**
3	• **Read** o **Chapter 6**:"Windows 2003/XP/2000 Addendum," DISA, 2005. http://www.thinkfreedocs.com/docs/popup.php?dsn=557746 (accessed June 8, 2006) o **Chapter 2:** Souppaya, Murugiah, Karen Kent. Guide to Computer Security Log Management. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf • **Lab 1 and 2** • **In-class Discussion 1** • **Research Assignment 1**
4	• **Read** o "Windows XP Security Checklist" (LabMice.net) http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm (June

	8, 2006) • **Start Project 1 Part A and Part B** • **In-class Discussion 1**
5	• **Read** ○ **Chapters 12 and 6:** "UNIX Security Technical Implementation Guide (STIG)," DISA, 2006. http://iase.disa.mil/stigs/stig/unix-stig-v5r1.pdf • **In-class Discussion 1**
6	• **Read** ○ "The 60 Minute Network Security Guide – First Steps towards a Secure Network Environment," Systems and Network Attack Center, NSA. 2002 http://www.nsa.gov/ia/_files/support/I33-011R-2006.pdf • **Case Assignment 1** • **Start Project 2** • **Lab 1**
7	• **Read** ○ Blossom, MountAraratt. "Firewall Penetration Testing," 2000. http://www.wittys.com/files/mab/fwpentesting.html (accessed June 8, 2006) ○ Burrows, Dave. "Penetration 101 - Introduction to becoming a Penetration Tester," 2002. http://www.sans.org/rr/whitepapers/testing/266.php (accessed June 8, 2006) ○ Burke, Joshua, Brad Hartselle, Brad Kneuven, and Bradley Morgan. "Wireless Security Attacks and Defenses," 2006. http://www.windowsecurity.com/whitepapers/Wireless-Security-Attacks-Defenses.html (accessed June 8, 2006) • **In-class Discussion 1**

	• **Start Project 3** • **Submit Project 1 (Part A and Part B)** • **Lab 1**

8	• **Read**
	  ○ Database Security Checklist and Guidance, “Security Technical Implementation Guides” (Information Assurance Support Environment) http://iase.disa.mil/stigs/content_pages/database_security.html
	  ○ Winner, Duane. “Making Your Network Safe for Databases,” 2002. http://www.sans.org/rr/whitepapers/application/24.php (accessed June 8, 2006)
	• **Research Assignment 1**

9	• **Read**
	  ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room >eCommerce> e-commerce and Defense in Depth
	  ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room>eCommerce>Inspection Grade Card for Conducting E-commerce
	  ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room>Application/Database Sec>Deploying a Secure Web Application: From a Coding Perspective
	  ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room>Auditing & Assessment>The Application Audit Process - A Guide for Information Security Professionals
	• **In-class Discussion 1**
	• **Lab 1**

	• Case Assignment 1 • Submit Project 3
10	• Read ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room> Intrusion Detection>Host-Based Intrusion Detection: An Overview of Tripwire and Intruder Alert ○ ITT Tech Virtual Library >School of Study>School of Information Technology>Recommended Links>General>SANS Institute Reading Room> Attacking Attackers>Honey Pots and Honey Nets - Security through Deception ○ Bayer, Jen. “Microsoft Audit Collection System (MACS - beta).”http://download.microsoft.com/documents/australia/WINDOWS/MACSOverview.doc, 2003. • Research Assignment 1 • In-class Discussion 1
11	Final Examination

INTENT/INTERFACE

In earlier courses, the students learned the requirements for conducting electronic commerce, the components of an IT infrastructure for conducting e-commerce, and the techniques to secure such infrastructure. In this course, the students will learn to verify if the security measures are operating as intended, through analysis of the system’s security configuration settings and the interpretation of the security audit data.

The students who take this course will be prepared to assist in planning and conducting internal security self-audits of e-commerce systems. The understanding of various components, their interactions, and implementation of their security mechanisms provide the foundation for further development of the students’ expertise and experience. Of significance is the exposure of the

students to freely available, disciplined, security and auditing guidance, compiled by numerous federal and professional organizations.

