IS312T
Information Security Essentials
[Onsite]

Course Description:

This course is an introduction to the security essentials. The course identifies and examines types of information security used in industry and how they are implemented.

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

Prerequisites: Basic courses in computer applications and functioning of operating systems

Credit hours: 4

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

SYLLABUS: Information Security Essentials

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

Upon successful completion of this course, the student will be able to discuss each of the 10 domains of the Common Body of Knowledge (CBK).

- Security Management Practices
- Access Control Systems
- LIE
- Security Architecture and Models
- Application and System Development
- Operations Security
- Cryptography
- BCP / DRP
- Telecommunications
- Physical Security

COURSE OBJECTIVES

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

1. Explain Information Security.

1.1 Define Information Security.

1.2 Explain importance of Information security.

1.3 Define Information Security terminology.

1.4 Define Risk analysis.

2. Identify the various threats to Information Security.

    2.1 Define threats.

    2.2 Identify the attackers of Information Security.

    2.3 Identify the types of attacks.

3. Explain the basic principles of Information Security.

    3.1 Describe who is responsible for Information Security.

    3.2 Identify effective authentication methods.

    3.3 Identify methods of control access to computer systems.

4. Describe a Security Baseline.

    4.1 Identify the methods used for hardening networks.

    4.2 Identify the methods used for hardening operating systems.

    4.3 Identify the methods used for hardening applications.

5. Explain the concept of a secure network infrastructure.

    5.1 Identify the resources in a network Infrastructure.

    5.2 Describe the process of hardening network devices.

    5.3 Describe secure network topologies.

    5.4 Describe the media and methods used to physically secure network infrastructure.

6. Identify the need for Web security.

    6.1 Describe the process of protecting E-Mail.

    6.2 Describe vulnerabilities in Web sites and Web based communications.

7. Describe how to protect advanced communications systems.

    7.1 Define secure remote access.

    7.2 Identify vulnerabilities in cellular telephony.

    7.3 Describe the hardening of wireless networks.

8. Explain the concept of Cryptography.

    8.1 Identify the various elements of cryptography.

    8.2 Define Hashing Algorithms.

9. Describe Public Key Infrastructure.

    9.1 Describe Digital Certificates.

    9.2 Explain the process of key management.

10. Describe Operational Security.

    10.1 Identify the need for physical security.

    10.2 Identify the need for business continuity planning.

    10.3 Identify the types of Backups.

    10.4 Identify the solutions used in disaster recovery.

11. Describe Policies and Procedures.

    11.1 Identify the need for risk management.

    11.2 Identify the tasks performed in the various phases of the risk management process.

    11.3 Define the types of security policy.

12. Explain Security Management Procedures.

    12.1 Define privilege management.

    12.2 Define change management.

    12.3 Explain Digital Rights Management (DRM).

    12.4 Identify the need for security awareness training.

13. Describe Computer Forensics.

    13.1 Define the uses of a computer forensics.

Related SCANS Objectives

1. Research various sources to acquire relevant information from various sources.
2. Organize the gathered information under predefined categories in a systematic fashion.
3. Articulate concepts in written and verbal forms.

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

- **Textbook**: Ciampa, Mark. *Security + Guide to Network Security Fundamentals Second* Edition. Canada: Course Technology, Thomson, 2005.
- **DVD**:
  - **Security+ LabSim**
- **CD ROM**:
  - A+ LabSim
- **Lab Manual**: Cretaro, Paul. Lab Manual for *Security + Guide to Network Security Fundamentals. Second Edition. Canada: Course Technology, Thomson, 2005.* *(download path: Virtual Library > School of Information Technology > Selected Textbooks > IS312)*

References and Resources

ITT Tech Virtual Library

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

- **Books**

The following book is related to this course and is available through the ITT Tech Virtual Library:

- Whitman, Michael. and Herbert Mattord. *Principles of Information Security. Second edition. Canada: Course Technology, 2005.*

Other Resources

- Internet

  - www.sans.org
  - www.cert.org
  - http://www.issa.org/
  - www.mcafee.com
  - www.fsecure.com
  - www.rms.com
  - www.rmis.com
  - http://www.hideaway.net/home/public_html/index.php
  - http://techrepublic.com.com/2001-1009_11-0.html
  - http://www.dataprotection.gov.uk/dpaudit/whatis/backgrnd/howfit.htm
  - http://www.nttdata.co.jp/en/media/2001/092600.html
  - http://qdn.qnx.com/support/docs/qnx4/utils/c/cpio.html

All links to Web references outside the ITT Tech Virtual Library are 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

Final grades will be based on the following weighted categories:

CATEGORY	WEIGHT
Participation	10%
Lab Assignments	25%
Quizzes	20%
Midterm Exam	20%
Final Exam	25%
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 ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 1, pp. 1-11 ▪ Chapter 2, pp. 29-52 • Writing Assignments: 1 and 2 • Class Activities: 1 and 2 • Quiz: 1 • Labs: 1. Also, refer to Labs in Appendix II
2.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 3, pp. 69-89 • Writing Assignments: 1 and 2 • Class Activities: 1 • Quiz: 1 • Labs: 1, 2, and 3. Also, refer to Labs in Appendix II
3.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 4, pp. 104-124 ▪ Chapter 5, pp. 1401-72 • Writing Assignments: 1 and 2 • Class Activities: 1

	• Quiz 1 • Labs: 1, 2, 3, 4, 5, 6, 7, and 8. Also, refer to Labs in Appendix II
4.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 6, 190-213 ▪ Chapter 7, pp. 226-255 • Writing Assignments: 1 and 2 • Class Activities: 1 and 2 • Quiz 1 • Labs: 1, 2, 3, 4, 5, 6, 7, 8, and 9. Also, refer to Labs in Appendix II.
5.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 8, pp. 272-294 • Writing Assignments: 1 and 2 • Class Activities: 1 and 2 • Quiz 1 • Labs: 1, 2, 3, 4, 5, 6, and 7. Also, refer to Labs in Appendix II
6.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 9, pp. 308-330 • Writing Assignments: 1, 2, and 3 • Class Activities: 1

	• Midterm Exam • Labs: 1, 2, 3, 4, 5, and 6. Also, refer to Labs in Appendix II
7.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 10, pp. 342-369 • Writing Assignments: 1 and 2 • Class Activities: 1 and 2 • Quiz 1 • Labs: 1, 2, and 3. Also, refer to Labs in Appendix II
8.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 11, pp. 382-406 • Writing Assignment: 1 • Class Activities: 1 and 2 • Quiz 1 • Labs: 1, 2, and 3. Also, refer to Labs in Appendix II
9.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 12, pp. 418-435 • Writing Assignments: 1 and 2 • Class Activities: 1 and 2

	• Quiz 1 • Labs: 1, 2, 3, and 4. Refer to Labs in Appendix II
10.	• Read ○ *Security + Guide to Network Security Fundamentals, Second Edition* ▪ Chapter 13, pp. 446-457 • Writing Assignments: 1 • Class Activities: 1 and 2 • Quiz 1 • Labs: 1, 2, 3, 4, 5, and 6. Also, refer to Labs in appendix II
11.	Final Exam

INTENT/INTERFACE

Security is the primary concern of current computer professionals, with good reason. The Slammer worm infected 75,000 computers within the first 11 minutes of its release. The number of computers infected doubled every 8.5 seconds. The Blaster worm infected 138,000 computers within the first four hours of its release. Of the more than 141 million online consumers in the United States, more than 57 million have received phishing e-mails. One out of every three computers connected to the Internet has unwanted software such as a Trojan horse or spyware installed. This course is designed to meet the needs of students and computer professionals who want to understand how to protect themselves from these dangers. It is an overview of the 10 security domains of the Common Body of Knowledge (CBK), as defined by the International Information Systems Security Certification Consortium $(ISC)^2$. As the students progress through the course, each domain will be examined in depth. This will help the students understand information security and prepare them for a career in the fast-paced and growing field of information technology.

