ITT Technical Institute

NT2580

Introduction to Information Security

Onsite Course

SYLLABUS

Credit hours: 4.5

Contact/Instructional hours: 56 (34 Theory Hours, 22 Lab Hours)

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

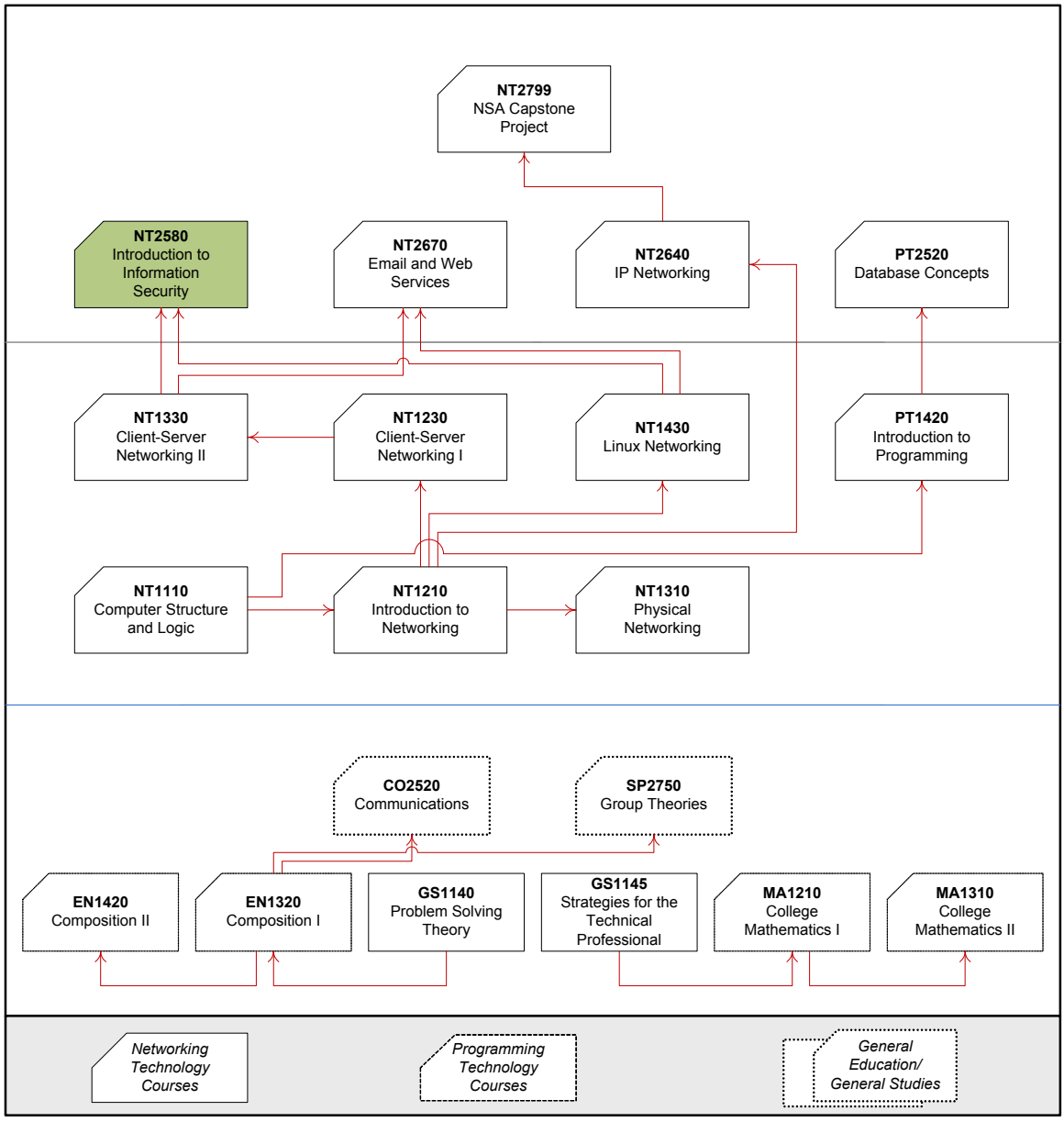
Prerequisites: NT1330 Client-Server Networking II or equivalent, NT1430 Linux Networking or equivalent

Course Description:

This course provides an overview of security challenges and strategies of counter measures in the information systems environment. Topics include definitions of terms, concepts, elements and goals incorporating industry standards and practices with a focus on availability, vulnerability, integrity and confidentiality aspects of information systems.

Where Does This Course Belong?

This course is required for the associate degree program in Network Systems Administration (NSA). The following diagram demonstrates how this course fits in the program:



Course Summary

Major Instructional Areas

1. Information Systems Security fundamentals
2. Seven domains of a typical Information Technology (IT) infrastructure
3. Risks, threats, and vulnerabilities found in a typical IT infrastructure
4. Security countermeasures for combating risks, threats, and vulnerabilities commonly found in an IT infrastructure
5. $(ISC)^2$ Systems Security Certified Practitioner (SSCP®) Common Body of Knowledge – SSCP® domains
6. Six domains of the CompTIA Security+ certification

Course Objectives

1. Explain the concepts of information systems security as applied to an IT infrastructure.
2. Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
3. Explain the role of access controls in implementing a security policy.
4. Explain the role of operations and administration in effective implementation of security policy.
5. Explain the importance of security audits, testing, and monitoring to effective security policy.
6. Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
7. Explain how businesses apply cryptography in maintaining information security.
8. Analyze the importance of network principles and architecture to security operations.
9. Explain the means attackers use to compromise systems and networks and defenses used by organizations.
10. Apply international and domestic information security standards and compliance laws to real-world implementation in both the private and public sector.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Kim, David, and Michael G. Solomon. *Fundamentals of Information Systems Security*. 1st ed. Sudbury, MA: Jones & Bartlett, 2010.	▪		

Recommended Resources

Professional Associations

The following is a list of vendor neutral professional organizations and their respective certifications:

- CISSP® and SSCP® Information Systems Security Certifications
  http://www.isc2.org/ (accessed April 28, 2014).
- CSIH Certification
  http://www.cert.org/ (accessed April 28, 2014).
- FISMA Training and Certification
  http://www.fismacenter.com/ (accessed April 28, 2014).
- SANS GIAC Certifications
  http://www.sans.org/ (accessed April 28, 2014).
- Security + Certification
  http://www.comptia.com/ (accessed April 28, 2014).

The following is a list of vendor-specific professional certifications:

- CCSP Certification
  http://www.cisco.com/ (accessed April 28, 2014).
- Check Point Firewall Specialist Certifications
  http://www.checkpoint.com/ (accessed April 28, 2014).
- MSCE Security Certification
  http://www.microsoft.com/ (accessed April 28, 2014).
- RSA Training and Certifications
  http://www.rsa.com/ (accessed April 28, 2014).

- Symantec Security Specialist Certifications
  http://www.symantec.com/ (accessed April 28, 2014).

Other References

- CVE List
  http://cve.mitre.org/ (accessed April 28, 2014).
- National Vulnerability Database
  http://nvd.nist.gov/ (accessed April 28, 2014).
- SANS Top 20 Threats/Vulnerabilities
  http://www.sans.org/top-cyber-security-risks/?ref=top20 (accessed April 28, 2014).
- CERT® Coordination Center
  http://www.cert.org/(accessed April 28, 2014).
- US Computer Emergency Readiness Team
  http://www.us-cert.gov/ (accessed April 28, 2014).
- US Department of Homeland Security
  http://www.dhs.gov/ (accessed April 28, 2014).
- US National Institute of Standards & Technology
  http://www.nist.gov/ (accessed April 28, 2014).

NOTE: All links are subject to change without prior notice.

Keywords:

- Availability
- Business Continuity
- Business Impact Analysis
- Compliance Laws
- Confidentiality
- Cryptography
- Disaster Recovery
- Incident Response
- Information Security
- Information Systems Security
- Integrity
- IT Risks, Threats, Vulnerabilities
- IT Security Assessment
- IT Security Audit
- Malicious Code

- Malware
- Network Security
- Risk Management
- Security Breaches
- Security Controls
- Security Countermeasures
- Security Incidents
- Security Management
- Security Monitoring
- Security Operations
- Security Testing
- Telecommunications Security
- Unauthorized Access

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to the development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Information Systems Security Fundamentals	*Fundamentals of Information Systems Security*: ▪ Chapter 1	Lab	1.1	Performing Reconnaissance and Probing using Common Tools (vLab)	2
			Assignment	1.2	Match Risks/Threats to Solutions	1
				1.3	Impact of a Data Classification Standard	1
2	Application of Security Countermeasures to Mitigate Malicious Attacks	*Fundamentals of Information Systems Security*: ▪ Chapter 3 ▪ Chapter 4	Lab	2.1	Performing a Vulnerability Assessment (vLab)	2
			Project	2.2	Project Part 1: Multi-Layered Security Plan†	6
			Assignment	2.3	Calculate the Window of Vulnerability	1
				2.4	Microsoft Environment Analysis	1
3	Appropriate Access Controls for Systems, Applications, and Data Access	*Fundamentals of Information Systems Security*: ▪ Chapter 5	Lab	3.1	Enabling Windows Active Directory and User Access Controls (vLab)	2
			Discussion	3.2	Access Control Models	4
			Assignment	3.3	Remote Access Control Policy Definition	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
4	Effective Implementation of Security Policy	*Fundamentals of Information Systems Security*: ▪ Chapter 6	Lab	4.1	Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control (vLab)	2
			Assignment	4.2	Enhance an Existing IT Security Policy Framework	1
				4.3	Acceptable Use Policy (AUP) Definition	1
5	Importance of Testing, Auditing, and Monitoring	*Fundamentals of Information Systems Security*: ▪ Chapter 7	Lab	5.1	Performing Packet Capture and Traffic Analysis (vLab)	2
			Assignment	5.2	Testing and Monitoring Security Controls	1
				5.3	Define an Acceptable Use Policy (AUP)	1
6	Role of Risk Management, Response, and Recovery for IT Systems, Applications, and Data	*Fundamentals of Information Systems Security*: ▪ Chapter 8	Lab	6.1	Implementing a Business Continuity Plan (vLab)	2
			Assignment	6.2	BCP, DRP, BIA, and Incident Response Plan Mix and Match	4
				6.3	Quantitative and Qualitative Risk Assessment Analysis	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
7	Role of Cryptography in Maintaining Confidentiality and Privacy of Data	*Fundamentals of Information Systems Security*: ▪ Chapter 9	Lab	7.1	Using Encryption to Enhance Confidentiality and Integrity (vLab)	2
			Assignment	7.2	Select Appropriate Encryption Algorithms	1
				7.3	Design an Encryption Strategy	1
8	Networks and Communications and their Inherent Weaknesses	*Fundamentals of Information Systems Security*: ▪ Chapter 10	Lab	8.1	Performing a Web site and Database Attack by Exploiting Identified Vulnerabilities (vLab)	2
			Assignment	8.2	Network Hardening	1
				8.3	Network Security Applications and Countermeasures	1
9	Mitigation of Risk and Threats from Attacks and Malicious Code	*Information Fundamentals of Information Systems Security*: ▪ Chapter 11	Lab	9.1	Eliminating Threats with a Layered Security Approach (vLab)	2
			Assignment	9.2	List Phases of a Computer Attack	1
				9.3	Summary Report on a Malicious Code Attack	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
10	Information Security Standards and Compliance Laws	*Information Security Fundamentals–What Every Information Security Practitioner Should Know*: ▪ Chapter 12 ▪ Chapter 15	Lab	10.1	Implementing an Information Systems Security Policy (vLab)	2
			Assignment	10.2	Examine Real-World Implementations of Security Standards and Compliance Laws	1
				10.3	Small- to Medium-Sized Business Analysis	4
11	Course Review and Final Examination	N/A	Project	11.1	Project Part 2: Student SSCP® Domain Research Paper†	15
			Exam	11.2	Final Exam	30

† Candidate for ePortfolio

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Assignment	25%
Lab	20%
Project	21%
Discussion	4%
Exam	30%
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage	Credit
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

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)