

FLORIDA STATE COLLEGE AT JACKSONVILLE

COLLEGE CREDIT COURSE OUTLINE

COURSE NUMBER: CET2687

COURSE TITLE: Security+

PREREQUISITE(S): None

COREQUISITE(S): None

CREDIT HOURS: 3

CONTACT HOURS/WEEK: 4

CONTACT HOUR BREAKDOWN:

Lecture/Discussion: 3

Laboratory: 1

Other _____:

FACULTY WORKLOAD POINTS: 3.7

STANDARDIZED CLASS SIZE
ALLOCATION: 24

CATALOG COURSE DESCRIPTION:

This course provides the fundamental knowledge necessary for a student to become proficient in the field of Information Security. Security+ is vendor-neutral and prepares the student for a wide variety of security responsibilities. The vendor neutral aspect of the curriculum allows the student to be immediately productive in today's diverse security industry, thereby reducing the normal length of internship required for new employees. The Fundamentals of Information Security curriculum covers a wide range of security concepts, including: General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography, and Operational and Organizational Security

SUGGESTED TEXT(S): Security+ Study Guide (Current edition) by Syngress

IMPLEMENTATION DATE: Spring Term, 2003 (20032)

REVIEW OR MODIFICATION DATE: Fall Term, 2008 (20091) Proposal 2008-19

COURSE TOPICS	CONTACT HOURS <u>PER TOPIC</u>
I. <i>General Security Concepts</i>	20
II. <i>Communications Security</i>	4
III. <i>Infrastructure Security</i>	8
IV. <i>Basics of Cryptology</i>	8
V. <i>Operational/Organizational Security</i>	4
VI. <i>Hands-on Lab</i>	8
VII. <i>Hands-on Tests</i>	8
Total:	<u>60</u>

PROGRAM TITLE: IT Security
COURSE TITLE: Security+
CIP NUMBER: 1506120106 AS

LIST PERFORMANCE STANDARD ADDRESSED:

05.0 Demonstrate an understanding of network access control systems and methodology-The student will be able to:

- 05.10 Analyze methods of server attack, including brute force, denial of service, spoofing, spamming, sniffers, hackers, and crackers
- 05.11 Demonstrate an understanding of the different types of intrusions and the different methods of intrusion detection, including data extraction, sampling, recognition and traffic analysis
- 05.12 Monitor the network using various forms of intrusion detection resources to detect attacks
- 05.13 Investigate audit trails for signs of network intrusions
- 05.14 Perform penetration testing to find weaknesses in the access control systems.

06.0 Describe cryptography concepts, standards, and applications-The student will be able to:

- 06.01 Demonstrate an understanding of the encryption/decryption process.
- 06.02 Demonstrate an understanding of the basic functions involved in key management including creation, distribution, verification, revocation, destruction, storage, recovery, and life span of keys.
- 06.03 Utilize various forms of cryptography, digital certificates, and digital signatures to achieve confidentiality, integrity, authentication, and non-repudiation in an enterprise data communications network.
- 06.04 Discuss the creation and use of digital certificates and digital signatures to provide authentication of users and verification of data integrity in network communications.
- 06.05 Employ cryptographic algorithms such as DES, RSA, MD5 and DSA.
- 06.06 Identify the strengths and weaknesses of cryptographic algorithms and the effects of key length.
- 06.07 Implement current popular key distribution methods including manual, Kerberos™, and Internet Security Association and Key Management Protocol (ISAKMP).
- 06.08 Utilize application and network-based protocols such as Secure Socket Layer (SSL), Secure HyperText Transfer Protocol (SHTTP), and Internetworking Protocol Security (IPSEC).
- 06.09 Describe the use of hardware components such as smart cards and tokens.

07.0 Perform telecommunications and network security activities - The student will be able to:

- 07.01 Utilize protocol layering models such as the Open Systems Interconnection (OSI) model in analyzing network security threats.
- 07.02 Evaluate the security implications involved with the various physical media types such as fiber optics, twisted pair, and wireless communications.
- 07.03 Describe security concerns with using certain network topologies such as star, bus, mesh, and ring.
- 07.05 Employ network monitors and packet sniffers to identify security threats.
- 07.07 Discuss the security vulnerabilities of the Transmission Control Protocol/Internetworking Protocol (TCP/IP) protocol stack.

LIST PERFORMANCE STANDARD ADDRESSED: (Continued)

- 10.0 Demonstrate an understanding of e-commerce-The student will be able to:
- 10.06 Discuss the steps necessary to maintain transaction integrity.
- 13.0 Design and implement physical security measures-The student will be able to:
- 13.01 Identify the physical threats to an enterprise's resources that include the employees, facilities, data, equipment, support systems, media, and supplies they utilize.
 - 13.02 Diagnose an enterprise's physical vulnerabilities to threats from natural disasters such as fire, flooding, and power loss.
 - 13.03 Specify possible countermeasures to physically protect an enterprise's resources and sensitive information.
 - 13.04 Develop a list of physical facility requirements to secure the premises.
 - 13.05 Evaluate the applicability of technical controls such as smart cards, access logs, and intrusion detection systems.
- 14.0 Perform operations and security management practices-The student will be able to:
- 14.08 Compare the advantages and disadvantages of internal versus external audits.
 - 14.10 Identify different types of monitoring including event, hardware, and illegal software.
 - 14.13 Perform penetration testing activities including sniffing, eavesdropping, dumpster diving, and social engineering.
 - 14.14 Understand principles of risk management and asset valuation.
- 15.0 Employ applications and systems development security techniques- The student will be able to:
- 15.06 Analyze local environment application issues including viruses, Trojan horses, logic bombs and worms.
 - 15.09 Compare different forms of data/information storage including primary, secondary, real, virtual, random, volatile, and sequential.
 - 15.11 Understand the difference between supervisory and user modes of operation.
 - 15.12 Identify various levels of application integrity including network, operating system, database, and file level integrity.
 - 15.13 Define the various types of computer viruses and malicious code and the roles that hackers, crackers, phreaks, and virus writers play in developing and utilizing malicious code.
- 17.0 Describe ethical issues, pertinent laws, and how to conduct investigations-The student will be able to:
- 17.01 Understand the major categories and types of laws as to how they relate to E-commerce, including criminal law, civil law and administrative law.
 - 17.03 Describe abnormal and suspicious activity as it relates to database and e-commerce security.
 - 17.04 Analyze potential data security threats such as fraud or collusion.
 - 17.06 Identify the major categories of computer crime and attacks, including military, business, financial, terrorist, grudge and "fun" attacks.
 - 17.08 Discuss major ethical and legal issues related to Internet use.

LIST PERFORMANCE STANDARD ADDRESSED: (Continued)

18.0 Perform general organizational computing workplace competencies- The student will be able to:

- 18.01 Follow oral and written instructions.
- 18.04 Participate in group discussions as a member and as a leader.
- 18.05 Interpret appropriate information from graphics, maps, or signs.
- 18.06 Demonstrate self-motivation and responsibility to complete an assigned task.
- 18.08 Identify and discuss issues contained within professional codes of conduct.
- 18.09 Identify and discuss intellectual property rights and licensing issues.
- 18.10 Identify potential sources of employee/employer or employee/employee conflict and discuss possible approaches to resolve such disagreements.

20.0 Perform documentation and technical reference activities- The student will be able to:

- 20.01 Use technical vocabulary appropriately
- 20.02 Locate information in printed and online technical references

PROGRAM TITLE: Networking Services Technology

COURSE TITLE: Fundamentals of Information Security

CIP NUMBER: 0615.040200 1507.030401 (AS) / 0507.030401 (AAS)

LIST PERFORMANCE STANDARD ADDRESSED:

NUMBER(S): TITLES(S):

01.0 Demonstrate understanding of networked environments - The student will be able to:

- 01.01 Explain the use of binary numbers to represent instructions and data.
- 01.03 Convert numbers among decimal, binary, and hexadecimal representation.
- 01.05 Identify various coding schemes (ASCII, etc.).
- 01.08 Describe current network environments, such as peer-to-peer and client/server.
- 01.09 Identify and discuss issues (such as security, privacy, redundancy, etc.) related to networked environments.
- 01.10 Identify and discuss issues related to naming conventions for user ids, email, passwords, and network devices.
- 01.11 List and define layers in the OSI and TCP/IP network protocol models.
- 01.12 Identify and describe current relevant IEEE network standards.
- 01.13 Illustrate typical network topologies.
- 01.17 Discuss the nature of IP addresses and MAC addresses, and mapping between protocol addressing schemes.
- 01.19 Identify and discuss technical issues related to emerging technologies (such as security, bandwidth capability, and gigabit transmission rates).
- 01.20 Discuss the design and function of a storage-area network (SAN).
- 01.22 Identify the advantages of VLANs.
- 01.23 Characterize a VLAN implementation.

02.0 Demonstrate understanding of data communications - The student will be able to:

- 02.13 Identify LAN access control methods (CSMA/CD, token passing, etc.).
- 02.14 Compare and contrast the major features of the LAN access methods.
- 02.17 Identify and describe file transfer protocols and methodologies.

05.0 Understand, install and configure network hardware - The student will be able to:

- 05.08 Recognize and describe current cable technologies such as twisted-pair, coaxial, and fiber optic, and identifying issues associated with plenum versus non-plenum cable plants.
- 05.09 Describe current wireless technologies such as satellite, microwave, spread spectrum RF, and infrared.
- 05.10 Identify advantages and disadvantages of wireless and cable technologies.
- 05.12 Describe the major functions of network connectivity hardware, such as hubs, repeaters, bridges, routers, switches, and gateways.
- 05.14 Describe the function of network storage devices and other peripherals (RAID, CD towers, printers, fax machines, scanners, printer/fax/copiers, imaging devices, and document center equipment, etc.).

LIST PERFORMANCE STANDARD ADDRESSED: (Continued)

07.0 Perform internetworking activities - The student will be able to:

- 07.01 Describe WAN topologies and MAN topologies.
- 07.02 Differentiate between WAN topologies and LAN topologies.
- 07.16 Explain the function and purpose of firewalls and firebreaks and their purpose.
- 07.18 Explain three major security concerns relating to data communications.

08.0 Perform Network administration and management activities - The student will be able to:

- 08.02 Establish, document and disseminate user security guidelines.
- 08.11 Document security policies and violations.
- 08.12 Install and update anti-virus software.
- 08.13 Describe current encryption standards - public vs. private key, NSA DES, PGP.
- 08.14 Describe the functions and characteristics of firewalls.
- 08.15 Address security issues raised by the ability to access server remotely.
- 08.16 Discuss the functions of authentication servers, RADIUS, and VPN.
- 08.17 Establish files backup procedures.
- 08.25 Establish a baseline for optimal network performance.

12.0 Demonstrate professional development skills - The student will be able to understand the importance of:

- 12.01 Attending classes, seminars, and workshops.
- 12.02 Reviewing literature and reading current literature.
- 12.03 Evaluating skills and taking necessary steps to upgrade.

14.0 Perform general organizational computing workplace competencies - The student will be able to:

- 14.01 Follow oral and written instructions.
- 14.10 Identify and discuss software-licensing issues.
- 14.11 Identify and discuss property rights and licensing issues.
- 14.12 Identify and discuss privacy issues.



NOTE: Use either the Tab key or mouse click to move from field to field. The box will expand to accommodate your entry.

Section 1	
COURSE PREFIX AND NUMBER: CET2687	SEMESTER CREDIT HOURS: 3
COURSE TITLE: Security+	

Section 2

TYPE OF COURSE: (Click on the box to check all that apply)

AA Elective AS Required Professional Course College Prep
 AS Professional Elective AAS Required Professional Course Technical Certificate
 Other _____
 General Education: (For General Education courses, you must also complete Section 3 and Section 7)

Section 3 (If applicable)

INDICATE BELOW THE DISCIPLINE AREA FOR GENERAL EDUCATION COURSES:

Communications Social & Behavioral Sciences Mathematics
 Natural Sciences Humanities

Section 4

INTELLECTUAL COMPETENCIES:

Reading Speaking Critical Analysis Quantitative Skills Scientific Method of Inquiry
 Writing Listening Information Literacy Ethical Judgment Working Collaboratively

Section 5		
	LEARNING OUTCOMES	METHOD OF ASSESSMENT
	<ul style="list-style-type: none"> The student demonstrates understanding of basic security principles including General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography and Operational and Organizational Security. 	Written assessment (Program Assessment requirement)
	<ul style="list-style-type: none"> The student demonstrates understanding of cryptography using tools such as JPHide and JPseek to perform Steganography. The student will create MD5 Hashes of files and observe their properties when altered. 	Written assessment
	<ul style="list-style-type: none"> The student describes Public Key Infrastructure by exploring various Browser programs and their Digital Certificate stores. The student will use tools such as CAPs to reinforce the concepts of Public/Private Key Cryptography. 	Written assessment
	<ul style="list-style-type: none"> The student compares and contrasts methods of Access Control, Authentication, and Auditing by demonstrating proficiency in AAA configuration. The student will be required to configure DAC Authentication and test the restrictions imposed by the configuration. 	Written assessment

Section 5 (Continued)

Section 5		METHOD OF ASSESSMENT
LEARNING OUTCOMES		
<ul style="list-style-type: none"> The student will recognize attacks on information systems using Ethereal or WireShark network analyzer and required to demonstrate its use in network attacks. The Student will be trained to use Network scanners such as Nmap and SuperScan to determine if a system is vulnerable to attack. 		Written assessment (E-portfolio requirement)
<ul style="list-style-type: none"> The student recognizes the dangers of Remote Access and E-mail using tools such as VNC and Terminal Services and to recognize the vulnerabilities inherent in Remote Access and E-Mail. 		Written assessment
<ul style="list-style-type: none"> The student explains basic Web security including how to properly configure Microsoft's Baseline Security and Internet Information Server Lockdown tools. 		Written assessment (E-portfolio requirement)
<ul style="list-style-type: none"> The student can use and understand basic Intrusion Detection Systems by configuring the open systems Intrusion Detection Tool SNORT. 		Written assessment
<ul style="list-style-type: none"> The student applies the basics of computer system Hardening including determination if a computer has been hardened for Internet use. 		Written assessment
<ul style="list-style-type: none"> The student demonstrates understanding of basic security principles including General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography and Operational and Organizational Security. 		Written assessment (Program Assessment requirement)
<ul style="list-style-type: none"> The student demonstrates understanding of cryptography using tools such as JPHide and JPseek to perform Steganography. The student will create MD5 Hashes of files and observe their properties when altered. 		Written assessment

Section 6 Name of Person Completing This Form: Cheryl SchmidtDate: 03/13/2008