Course Acronym:	ECHT
Course Number:	148
Descriptive Title:	CompTIA Security+ Computer Hardware Systems
Division:	Industry and Technology
Department:	Electronics and Computer Hardware Technology
Course Disciplines:	Electronic Technology, Electronics
Catalog Description:	This course is designed for the student pursuing a career as a computer service technician. Students will develop the skills and knowledge required for passing the CompTIA Security+ Certification exam. Topics include information security, system threats and risks, protecting systems, network vulnerabilities, network defenses, wireless network security, security audits and policies, cryptographic methods, and the basics of computer forensics. Note: *Transfer limitations apply. Letter grade or pass/no pass option. (formerly Electronics and Computer Hardware Technology 148ab)
Prerequisite:	
Co-requisite:	
Recommended Preparation:	Electronics and Computer Hardware Technology 140
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	4
Outside Study Hours:	4
Total Course Hours:	108
Course Units:	3
Grading Method:	Letter Grade and Pass/No Pass
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	02/16/2010
Transfer UC:	No
Effective Date:	
General Education: ECC	
Term:	

Other:	
CSU GE:	
Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1 Course Notebook** The students will assemble and maintain a five-section course notebook. **SLO #2 Information Security** Students will demonstrate their knowledge of information security, system threats and risks, protecting systems, network vulnerabilities, network defenses, wireless network security, security audits and policies, cryptographic methods, and the basics of computer forensics. **SLO #3 Cybersecurity** Students will demonstrate their knowledge of "Chain of Custody" handling procedures of physical evidence in matters of cybersecurity.
Course Objectives:	1. Analyze proper procedures for installing and configuring security system components and devices. 2. Diagnose and troubleshoot computer system security problems and determine whether they are hardware or software related. 3. Identify security procedures, system threats and risks, and preventative security methods. 4. Compare and contrast hardware and software based attacks as they pertain to network systems. 5. Identify the main components of public key infrastructure system. 6. Define secure networking concepts and secure networking hardware components. 7. Set up a computer system to function in a secure network environment. 8. Differentiate between effective and ineffective security procedures in relationship to customers and employees.
Major Topics:	**I. OVERVIEW OF THE COMPTIA SECURITY+ EXAM (1 hour, lecture)** A. History of computer security B. Information security systems **II. THE COMPTIA SECURITY+ EXAM (2 hours, lab)** A. History of computer security B. Information security systems **III. INTRODUCTION TO SECURITY (2 hours, lecture)**

A. Information security
B. Attacks and defenses

IV. INTRODUCTION TO SECURITY (2 hours, lab)

A. Information security
B. Attacks and defenses

V. SYSTEM THREATS AND RISKS (2 hours, lecture)

A. Hardware-based attacks
B. Software-based attacks

VI. SYSTEM THREATS AND RISKS (4 hours, lab)

A. Hardware-based attacks
B. Software-based attacks

VII. PROTECTING SYSTEMS (4 hours, lecture)

A. Hardening the Operating System (OS)
B. Preventing systems from attacks
C. Protecting systems from attacks

VIII. PROTECTING SYSTEMS (8 hours, lab)

A. Hardening the OS
B. Preventing systems from attacks
C. Protecting systems from attacks

IX. NETWORK VULNERBILITIES AND ATTACKS (2 hours, lecture)

A. Network vulnerabilities
B. Types of attacks
C. Methods of attacks

X. NETWORK VULNERBILITIES AND ATTACKS (4 hours, lab)

A. Network vulnerabilities
B. Types of attacks
C. Methods of attacks

XI. NETWORK DEFENSES (2 hours, lecture)

A. Creating a secure network
B. Network security hardware devices

XII. NETWORK DEFENSES (4 hours, lab)

A. Creating a secure network
B. Network security hardware devices

XIII. AUTHENTICATION (2 hours, lecture)

A. Authentication fundamentals
B. Credentials and protocols
C. Remote security

XIV. AUTHENTICATION (4 hours, lab)

A. Authentication fundamentals
B. Credentials and protocols
C. Remote security

XV. WIRELESS NETWORK SECURITY (2 hours, lecture)

A. Wireless network vulnerabilities
B. Wireless network protection

XVI. WIRELESS NETWORK SECURITY (4 hours, lab)

A. Wireless network vulnerabilities
B. Wireless network protection

XVII. ACCESS CONTROL FUNDAMENTALS (2 hours, lecture)

A. Access control methods
B. Logical access control
C. Physical access control

XVIII. ACCESS CONTROL FUNDAMENTALS (4 hours, lab)

A. Access control methods
B. Logical access control
C. Physical access control

XIX. VULNERABILITY ASSESSMENTS (2 hours, lecture)

A. Risk management
B. Identifying vulnerabilities

XX. VULNERABILITY ASSESSMENTS (4 hours, lab)

A. Risk management
B. Identifying vulnerabilities

XXI. SECURITY AUDITS (2 hours, lecture)

A. Privilege auditing
B. Usage auditing
C. Monitoring tools

XXII. SECURITY AUDITS (4 hours, lab)

A. Privilege auditing
B. Usage auditing
C. Monitoring tools

XXIII. BASIC CRYPTOGRAPHY (6 hours, lecture)

A. Cryptography
B. Cryptographic algorithms
C. Disk and file cryptography

XXIV. BASIC CRYPTOGRAPHY (8 hours, lab)

A. Cryptography
B. Cryptographic algorithms
C. Disk and file cryptography

XXV. CRYPTOGRAPHIC METHODS (2 hours, lecture)

A. Digital certificates
B. Public Key Infrastructure (PKI)
C. Key management

XXVI. CRYPTOGRAPHIC METHODS (4 hours, lab)

A. Digital certificates
B. PKI
C. Key management

XXVII. BUSINESS CONTINUITY (2 hours, lecture)

A. Environmental controls
B. Redundancy planning
C. Disaster recovery
D. Computer forensics incident reporting

XXVIII. BUSINESS CONTINUITY (4 hours, lab)

A. Environmental controls
B. Redundancy planning
C. Disaster recovery

XXIX. SECURITY POLICIES AND TRAINING (2 hours, lecture)

A. Security policies
B. Types of security policies
C. Education and training

XXX. SECURITY POLICIES AND TRAINING (2 hours, lab)

A. Security policies

	B. Types of security policies C. Education and training **XXXI. SEMESTER PROJECT DEVELOPMENT (1 hour, lecture)** A. Critical analysis B. Individual and group discussion C. Outlining template for term project **XXXII. SEMESTER PROJECT DEVELOPMENT (10 hours, lab)** A. Critical analysis B. Individual and group discussion C. Presentation of term project
Total Lecture Hours:	36
Total Laboratory Hours:	72
Total Hours:	108
Primary Method of Evaluation:	3) Skills demonstration
Typical Assignment Using Primary Method of Evaluation:	After installing a new computer system, the system will not logon to the network. On a one-page lab report, list three possible security-related reasons that cause system's failure to logon to the network. Submit lab report to the instructor.
Critical Thinking Assignment 1:	Provided with a computer system with a suspected security policy infraction, perform a computer forensic investigation. Report findings on a two-page lab report and submit to the instructor.
Critical Thinking Assignment 2:	A customer installed firewall is not working properly. Diagnose the fault and configure the firewall for proper operation. Consult instructor for evaluation.
Other Evaluation Methods:	Performance Exams Objective Exams Other Exams Quizzes Reading Reports Written Homework Laboratory Reports Class Performance Homework Problems Term or Other Papers Multiple Choice Completion Matching Items True/False Other (specify): Security System Design Research Assignment
Instructional Methods:	Demonstration Discussion Group Activities Guest Speakers Laboratory Lecture

	Multimedia Presentations Other (please specify): Computer Based Training (CD-ROM software for enhanced student training)
If other:	
Work Outside of Class:	Study Answer questions Skill practice Required reading Problem solving activities Written work
If Other:	
Up-To-Date Representative Textbooks:	Mark Ciampa. CompTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS. 9th edition. Cengage Learning. 2022. Mark Ciampa. LAB MANUAL FOR SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS. 9th edition, Cengage Learning, 2022.
Alternative Textbooks:	
Required Supplementary Readings:	
Other Required Materials:	Compact Disk Read Only Memory (CD-ROM) Digital Versatile Disc-Read Only Memory (DVD-ROM) 1 USB Flash Drive of at least 8GB of storage 1 - 3 Ring Binder - 1 1/2" hard cover
Requisite:	
Category:	
Requisite course(s): List both prerequisites and corequisites in this box.	
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	
Requisite Skill:	
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	
Requisite course:	Electronics and Computer Hardware Technology 140
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**Understand computer system design and operational concepts.** ECHT 140 - Understand the operating principals of computer system hardware. **Understand analog and digital concepts involving computer systems.** ECHT 140 - Understand the operating principals of computer system hardware.

	Assemble and disassemble personal computer systems and install operating system software. ECHT 140 - Assemble and disassemble computer systems using industry standard techniques and safety procedures.
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Osanne Ugya
Date:	09/01/1989
Original Board Approval Date:	03/12/1990
Last Reviewed and/or Revised by:	Paul Akhigbe
Date:	01/05/2023
Last Board Approval Date:	07/17/2023 effective FALL 2024