El Camino College
COURSE OUTLINE OF RECORD – Approved

I. GENERAL COURSE INFORMATION

Subject and Number: **Electronics and Computer Hardware Technology 148**
Descriptive Title: **CompTIA Security+ Certification Preparation for Computer Hardware Systems**
Course Disciplines: **Electronics AND Electronic Technology**
Division: **Industry and Technology**

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: Letter grade or pass/no pass option.

Conditions of Enrollment:
Recommended Preparation: Electronics and Computer Hardware Technology 140

Course Length:	**X Full Term**	**Other (Specify number of weeks):**
Hours Lecture:	**2.00 hours per week**	**TBA**
Hours Laboratory:	**4.00 hours per week**	**TBA**
Course Units:	**3.00**	

Grading Method: **Both**
Credit Status **Associate Degree Credit**

Transfer CSU: **X Effective Date: 2/16/2010**
Transfer UC: **No**

General Education:

El Camino College:

CSU GE:

IGETC:

II. OUTCOMES AND OBJECTIVES

A. COURSE STUDENT LEARNING OUTCOMES (The course student learning outcomes are listed below, along with a representative assessment method for each. Student learning outcomes are not subject to review, revision or approval by the College Curriculum Committee)

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 Cyber security
Students will demonstrate their knowledge of "Chain of Custody" handling procedures of physical evidence
in matters of cyber security.

The above SLOs were the most recent available SLOs at the time of course review. For the most current SLO statements, visit the El Camino College SLO webpage at http://www.elcamino.edu/academics/slo/.

B. Course Student Learning Objectives (The major learning objective for students enrolled in this course are listed below, along with a representative assessment method for each)

1. Analyze proper procedures for installing and configuring security system components and devices.
   - Laboratory reports
2. Diagnose and troubleshoot computer system security problems and determine whether they are hardware or software related.
   - Laboratory reports
3. Identify security procedures, system threats and risks, and preventative security methods.
   - Objective Exams
4. Compare and contrast hardware and software based attacks as they pertain to network systems.
   - Written homework
5. Identify the main components of public key infrastructure system.
   - Objective Exams
6. Define secure networking concepts and secure networking hardware components.
   - Objective Exams
7. Set up a computer system to function in a secure network environment.
   - Laboratory reports
8. Differentiate between effective and ineffective security procedures in relationship to customers and employees.
   - Term or other papers

III. OUTLINE OF SUBJECT MATTER (Topics are detailed enough to enable a qualified instructor to determine the major areas that should be covered as well as ensure consistency from instructor to instructor and semester to semester.)

Lecture or Lab	Approximate Hours	Topic Number	Major Topic
Lecture	1	I	OVERVIEW OF THE COMPTIA SECURITY+ EXAM A. History of computer security B. Information security systems
Lab	2	II	THE COMPTIA SECURITY+ EXAM A. History of computer security B. Information security systems
Lecture	2	III	INTRODUCTION TO SECURITY A. Information security B. Attacks and defenses
Lab	2	IV	INTRODUCTION TO SECURITY A. Information security B. Attacks and defenses
Lecture	2	V	SYSTEM THREATS AND RISKS A. Hardware-based attacks B. Software-based attacks
Lab	4	VI	SYSTEM THREATS AND RISKS A. Hardware-based attacks B. Software-based attacks
Lecture	4	VII	PROTECTING SYSTEMS A. Hardening the Operating System (OS) B. Preventing systems from attacks C. Protecting systems from attacks
Lab	8	VIII	PROTECTING SYSTEMS A. Hardening the OS B. Preventing systems from attacks C. Protecting systems from attacks
Lecture	2	IX	NETWORK VULNERBILITIES AND ATTACKS A. Network vulnerabilities B. Types of attacks C. Methods of attacks
Lab	4	X	NETWORK VULNERBILITIES AND ATTACKS A. Network vulnerabilities B. Types of attacks C. Methods of attacks
Lecture	2	XI	NETWORK DEFENSES A. Creating a secure network B. Network security hardware devices

Lab	4	XII	NETWORK DEFENSES A. Creating a secure network B. Network security hardware devices
Lecture	2	XIII	AUTHENTICATION A. Authentication fundamentals B. Credentials and protocols C. Remote security
Lab	4	XIV	AUTHENTICATION A. Authentication fundamentals B. Credentials and protocols C. Remote security
Lecture	2	XV	WIRELESS NETWORK SECURITY A. Wireless network vulnerabilities B. Wireless network protection
Lab	4	XVI	WIRELESS NETWORK SECURITY A. Wireless network vulnerabilities B. Wireless network protection
Lecture	2	XVII	ACCESS CONTROL FUNDAMENTALS A. Access control methods B. Logical access control C. Physical access control
Lab	4	XVIII	ACCESS CONTROL FUNDAMENTALS A. Access control methods B. Logical access control C. Physical access control
Lecture	2	XIX	VULNERABILITY ASSESSMENTS A. Risk management B. Identifying vulnerabilities
Lab	4	XX	VULNERABILITY ASSESSMENTS A. Risk management B. Identifying vulnerabilities
Lecture	2	XXI	SECURITY AUDITS A. Privilege auditing B. Usage auditing C. Monitoring tools
Lab	4	XXII	SECURITY AUDITS A. Privilege auditing B. Usage auditing C. Monitoring tools
Lecture	6	XXIII	BASIC CRYPTOGRAPHY A. Cryptography B. Cryptographic algorithms C. Disk and file cryptography

Lab	8	XXIV	BASIC CRYPTOGRAPHY A. Cryptography B. Cryptographic algorithms C. Disk and file cryptography
Lecture	2	XXV	CRYPTOGRAPHIC METHODS A. Digital certificates B. Public Key Infrastructure (PKI) C. Key management
Lab	4	XXVI	CRYPTOGRAPHIC METHODS A. Digital certificates B. PKI C. Key management
Lecture	2	XXVII	BUSINESS CONTINUITY A. Environmental controls B. Redundancy planning C. Disaster recovery D. Computer forensics incident reporting
Lab	4	XXVIII	BUSINESS CONTINUITY A. Environmental controls B. Redundancy planning C. Disaster recovery
Lecture	2	XXIX	SECURITY POLICIES AND TRAINING A. Security policies B. Types of security policies C. Education and training
Lab	2	XXX	SECURITY POLICIES AND TRAINING A. Security policies B. Types of security policies C. Education and training
Lecture	1	XXXI	SEMESTER PROJECT DEVELOPMENT A. Critical analysis B. Individual and group discussion C. Outlining template for term project
Lab	10	XXXII	SEMESTER PROJECT DEVELOPMENT A. Critical analysis B. Individual and group discussion C. Presentation of term project
Total Lecture Hours		36	
Total Laboratory Hours		72	
Total Hours		108	

IV. PRIMARY METHOD OF EVALUATION AND SAMPLE ASSIGNMENTS

A. PRIMARY METHOD OF EVALUATION:

Skills demonstrations

B. 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.

C. COLLEGE-LEVEL CRITICAL THINKING ASSIGNMENTS:

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.

A customer installed firewall is not working properly. Diagnose the fault and configure the firewall for proper operation. Consult instructor for evaluation.

D. OTHER TYPICAL ASSESSMENT AND 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

V. INSTRUCTIONAL METHODS

Demonstration
Discussion
Group Activities
Guest Speakers
Laboratory
Lecture
Multimedia presentations
Other (please specify)
This is an in-class assignment. Computer Based Training (CD-ROM software for enhanced student training)

Note: In compliance with Board Policies 1600 and 3410, Title 5 California Code of Regulations, the Rehabilitation Act of 1973, and Sections 504 and 508 of the Americans with Disabilities Act, instruction delivery shall provide access, full inclusion, and effective communication for students with disabilities.

VI. WORK OUTSIDE OF CLASS

Study
Answer questions
Skill practice
Required reading
Problem solving activities
Written work

Estimated Independent Study Hours per Week: 4

VII. TEXTS AND MATERIALS

A. UP-TO-DATE REPRESENTATIVE TEXTBOOKS

Mark Ciampa. CompTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS.
5th ed. Cengage Learning, 2015.
Mark Ciampa. LAB MANUAL FOR SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS.
5th ed. Cengage Learning, 2015.

B. ALTERNATIVE TEXTBOOKS

C. REQUIRED SUPPLEMENTARY READINGS

Barrett, Weiss, Hausman, CompTIA Security+ SYO-401 Exam Cram, 5th ed. Pearson IT Certification, 2015.

D. OTHER REQUIRED MATERIALS

2 Blank CD-RW disks
4 Blank DVD-RW disks
1 USB Flash Drive of at least 2GB of storage
1 - 3 Ring Binder - 1 1/2" hard cover

VIII. CONDITIONS OF ENROLLMENT

A. Requisites (Course and Non-Course Prerequisites and Corequisites)

Requisites	Category and Justification

B. Requisite Skills

Requisite Skills

C. Recommended Preparations (Course and Non-Course)

Recommended Preparation	Category and Justification
Course Recommended Preparation Electronics and Computer Hardware Technology 140 or equivalent	
Non-Course Recommended Preparation Equivalent	If students have not taken ECHT 140 but have taken a similar course at another college or have understanding of basic computer hardware technology, they will be prepared to enroll in this course. It is recommended that students

	have basic computer hardware knowledge or they may not succeed in this class.

D. Recommended Skills

Recommended Skills
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.

E. Enrollment Limitations

Enrollment Limitations and Category	Enrollment Limitations Impact

Course created by Osanne Ugya on 09/01/1989

BOARD APPROVAL DATE: 03/12/1990

LAST BOARD APPROVAL DATE: 06/17/2019

Last Reviewed and/or Revised by STEVE COCCA **Date: March 6, 2019**

19868