Course Information Form (CIF)

Course Code: CSC 251

Course Title: Advanced Topics in Computer Security

Department: Business/Computer Science and Technologies
Effective Date: Summer 2026
PCS Code: 1.2 - Occupational/Technical Instruction
CIP Code: 11.0901
Repeatability: 0

Credit Hours

Catalog Notation: 2-2-3
Credit Hour Distribution:

Lecture: 2	Lab: 2	Clinical: 0	**Total: 3**

General Course Information

Catalog Description

Advanced topics in securing local area networks, authentication methods, operating system software, application and server software, and networked communications. Upon completion of course students should be prepared to pass Comp TIA Security+ certification exam.

General Course Objectives

Students will learn to manage security of all networked components of modern computing systems.

Minimum Placement Levels

English	Reading	Math
None	None	None

Prerequisites

Credit in CSC 130, and credit in CSC 153 or CSC 171

Methods of Evaluation

20 lab simulations, 23 virtual machine labs, 15 quizzes, 4 exams, and a final assessment exam.

Instructional Materials and Additional Supplies

CompTIA Security+ Guide to Network Security Fundamentals, 7th edition. 9780357424414

Course Content

General Learning Outcomes (GLOs)

- Critical Thinking and Information Literacy: Students will demonstrate the ability to evaluate perspectives, evidence, and implications, and to locate, assess, and use information effectively.
- Technology: Students will demonstrate the ability to evaluate, select, and appropriately use current and emerging tools.

Course Segments and Student Learning Outcomes

Course Segment	Learning Outcomes	Lecture Hours	Lab Hours	Clinical Hours
Introduction to Security	1. Describe the challenges of securing information; define information security, actors, and defending against threats. 2. Apply information security and threat mitigation principles.	2	2	0
Malware and Social Engineering Attacks	1. Define attacks that use malware and social engineering. 2. Apply defense strategies against attacks that use malware and social engineering.	2	2	0
Basic Cryptography	1. Define cryptography, cryptographic algorithms, cryptographic attacks, and how cryptography is used. 2. Apply techniques related to cryptography, cryptographic algorithms, and cryptographic attacks.	2	2	0
Advanced Cryptography and PKI	1. Describe the implementation of cryptography, digital certificates, public key infrastructure, and cryptographic transport protocols. 2. Implement cryptography, digital certificates, public key infrastructure, and cryptographic transport protocols.	2	2	0
Networking and Server Attacks	1. Describe networking-based attacks and server attacks. 2. Apply defense strategies against networking-based attacks and server attacks.	2	2	0
Network Security Devices, Design, and Technology	1. Describe security threats through network devices, network architecture, and network technologies. 2. Apply defense strategies against security threats through network devices, network architecture, and network technologies.	2	2	0
Administering a Secure Network	1. Describe secure network protocols, security devices and technologies, analyzing security data, and managing secure network platforms. 2. Apply secure network protocols, utilize security devices and technologies, analyze security data, and manage secure network platforms.	2	2	0
Wireless Network Security	1. Describe wireless attacks, security vulnerabilities, and wireless security solutions. 2. Apply defense strategies against wireless attacks, protect security vulnerabilities, and implement wireless security solutions.	2	2	0
Client and Application Security	1. Define client security, physical security, and application security. 2. Apply strategies for client security, physical security, and application security.	2	2	0
Mobile and Embedded Device Security	1. Describe mobile device deployment, mobile device risk, securing mobile devices, embedded systems, and the Internet of Things. 2. Apply strategies for mobile device deployment, mobile device risk, securing mobile devices, embedded systems, and the Internet of Things.	2	2	0

Course Segment	Learning Outcomes	Lecture Hours	Lab Hours	Clinical Hours
Authentication and Account Management	1. Define authentication credentials, Single Sign-on, and account management. 2. Implement authentication credentials and Single Sign-on, and manage accounts.	2	2	0
Access Management	1. Define access control; account management; best practices for access control; and implementation of access control, identity, and access services. 2. Apply strategies for access control and account management, including best practices, and implement access control, identity, and access services.	2	2	0
Vulnerability Assessment and Data Security	1. Describe vulnerability assessment, vulnerability scanning, penetration testing, and data privacy and security. 2. Apply strategies for vulnerability assessment, vulnerability scanning, penetration testing, and data privacy and security.	2	2	0
Business Continuity	1. Define business continuity, fault tolerance, environmental controls, and incident response. 2. Apply strategies for business continuity, fault tolerance, environmental controls, and incident response.	2	2	0
Risk Mitigation	1. Describe managing risk, reducing risk, practices for reducing risk, and troubleshooting common security issues. 2. Apply strategies for managing risk, reducing risk, and troubleshooting common security issues.	2	2	0

Total Contact Hours

Lecture Hours	Lab Hours	Clinical Hours
30	30	0