GROSSMONT COLLEGE

Official Course Outline

COMPUTER SCIENCE INFORMATION SYSTEMS 263 – SECURITY+ CERTIFICATION

1. Course Number Course Title Semester Units Semester Hours

CSIS 263 Security+ Certification 3 2 hours lecture: 32-36 hours

3 hours lab: 48-54 hours

64-72 outside-of-class hours

for lecture

144-162 total hours

2. Course Prerequisites

None

Corequisite

None

Recommended Preparation

A “C” grade or higher or “Pass” in CSIS 125 or equivalent.

3. Catalog Description

Entry-level course in network security that addresses the various aspects of designing and implementing a secure network. Designed for students interested in understanding the field of network security and how it relates to other areas of Information Technology (IT). Covers materials included in the CompTIA (Computing Technology Industry Association) Security+ exam.

4. Course Objectives

The student will:

1. Implement security configuration parameters on network devices.
2. Analyze the costs of intrusion into an organization’s computer system.
3. Compare and contrast the function and purpose of authentication services.
4. Demonstrate and set up secure remote access to access information.
5. Utilize operating system security and implement web security.
6. Implement the appropriate controls to ensure data security.

5. Instructional Facilities

Standard computer lab with one internet-connected workstation per student with appropriate software installed.

6. Special Materials Required of Student

Flash/USB drive or cloud storage for backup of in-class work.

COMPUTER SCIENCE INFORMATION SYSTEMS 263 – SECURITY+ CERTIFICATION Page 2

7. Course Content

a. Network Security foundational principles on network device components and configuration, administration policies, implementing common protocols and services and troubleshooting wireless networking.

b. Compliance and Operational Security to include basic risk assessment and risk management, security control selection, mitigation strategies, forensics, and incident response.

c. Threats and Vulnerabilities overview of types of malware, types of attacks, attack mitigation techniques, and vulnerability testing.

d. Application, Data and Host Security concepts including application security controls, mobile security, and host security.

e. Access Control and Identity Management fundamental concepts of authentication services, Service selection, and account management best practices.

f. Cryptography topics to include cryptography, cryptographic methods, PKI and certificate management components.

8. Method of Instruction

a. Online computer-based reading assignments

b. Lecture and demonstration in a traditional classroom or via electronic means

c. Hands-on practice in either a dedicated or a virtual lab environment

d. Topical discussion of current operating system trends and issues

9. Methods of Evaluating Student Performance

a. Written quizzes and exams including a final that measure students’ ability to describe computer security principles, functions and characteristics; analyze a scenario and choose the alternatives and troubleshooting options.

b. Scenario-based lab activities that measure students’ ability to configure specific computer security functions or subsystems, troubleshoot/analyze imposed security problems, investigate potential alternatives, and implement corrective action to achieve a determined result.

c. Practical application-based examinations that measure students’ ability to evaluate scenario-based computer security requirements/problems, analyze/troubleshoot the security configuration, and apply the correct configuration changes to achieve the correct results.

10. Outside Class Assignments

a. Complete study guides provided covering major topics.

b. Utilizing virtual machines configured with windows and windows server operating systems:

c. Configure specific computer security functions and/or subsystems.

d. Troubleshoot/analyze imposed security problems, investigate potential alternatives, and implement corrective action to achieve a determined result.

e. Complete and pass section quizzes and course final exam.

f. Read and analyze instructor assigned case studies; post analysis and comments to the class discussion board.

g. Respond to other students’ analysis and comments on the class discussion board.

11. Texts

a. Required Text(s):

Ciampa, M. *CompTIA Security+ Guide to Network Security Fundamentals.* 6th ed., Boston, MA: Cengage Learning, 2017.

b. Supplemental texts and workbooks:

None

COMPUTER SCIENCE INFORMATION SYSTEMS 263 – SECURITY+ CERTIFICATION Page 3

Addendum: Student Learning Outcomes

Upon successful completion of this course, our students will be able to do the following:

a. Define network security, network topologies, security threat trends, goals of network security, and factors in a comprehensive secure network strategy.

b. Describe in detail authentication with strong passwords, Kerberos, CHAP digital certificates, tokens and biometrics.

c. Describe in detail various forms of computer attacks, major types of malicious software, consequences and types of social-engineering and at least one countermeasure for each.

d. Illustrate the security implications, vulnerabilities, and common exploits associated with remote access and telecommuting technologies, scripting software, web applications, web-hosted applications, file and print sharing services.

e. Configure server, client and network security software, protocols, encryption, remote access technologies, authentication and authorization services, intrusion detection services, and equipment.

f. Conduct a security assessment. Define, document and develop a plan that addresses the security requirements for the organization, security policies, security topology, risk management, identified vulnerabilities, auditing requirements, and penetration testing.

Date approved by the Governing Board: May 21, 2019