Curriculum Committee Approval: 04/02/19

Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 263 – FUNDAMENTALS OF NETWORK SECURITY

2 hours lecture, 3 hours laboratory, 3 units

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.

Prerequisite
None

Recommended Preparation
"C" grade or higher or "Pass" in CIS 125 or 201 or equivalent, and "C" grade or higher or "Pass" in 190 or 191 or equivalent

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Comprehensive knowledge of computer hardware and operating systems.
2) Understanding basic networking, TCP/IP protocols and network command-line interface troubleshooting tools.
3) Diagnose and troubleshoot personal computer, install and patch an operating system on a personal computer.
4) Attach hardware peripherals and install appropriate driver software.

Course Content
1) Network Security foundational principles on network device components and configuration, administration policies, implementing common protocols and services and troubleshooting wireless networking.
2) Compliance and Operational Security to include basic risk assessment and risk management, security control selection, mitigation strategies, forensics, and incident response.
3) Threats and Vulnerabilities overview of types of malware, types of attacks, attack mitigation techniques, and vulnerability testing.
4) Application, Data and Host Security concepts including application security controls, mobile security, and host security.
5) Access Control and Identity Management fundamental concepts of authentication services, Service selection, and account management best practices.
6) Cryptography topics to include cryptography, cryptographic methods, PKI and certificate management components.

Course Objectives
Students will be able to:
1) Implement security configuration parameters on network devices, use secure network administration policies, explain network design elements and components, implement common protocols and services, and troubleshoot security issues related to wireless networking.

2) Explain the importance of risk related concepts, summarize the security implications of integrating systems and data with third parties, implement appropriate risk mitigation strategies, implement basic forensic procedures, summarize common incident response procedures, explain the importance of security related awareness training, compare and contrast physical security and environmental controls, summarize risk management best practices, and select the appropriate control to meet the goals of security.
3) Explain types of malware, summarize various types of attacks, summarize social engineering attacks and the associate effectiveness with each attack, explain types of wireless attacks, explain types of application attacks, analyze a scenario and select the appropriate type of mitigation and deterrent techniques, use appropriate tools and techniques to discover security threats and vulnerabilities, and explain the proper use of penetration testing versus vulnerability scanning.
4) Explain the importance of application security controls and techniques, summarize mobile security concepts and technologies, select the appropriate solution to establish host security, implement the appropriate controls to ensure data security, and compare and contrast alternative methods to mitigate security risks in static environments.
5) Compare and contrast the function and purpose of authentication services, select the appropriate authentication, authorization or access control, and install and configure security controls when performing account management based on best practices.
6) Utilize general cryptography concepts, use appropriate cryptographic methods, and use appropriate PKI, certificate management and associated components.

Method of Evaluation

A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.

1) Written quizzes and exams that measure students' ability to describe computer security principles, functions and characteristics; analyze a scenario and choose the alternatives and troubleshooting options.
2) 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.
3) 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.

Special Materials Required of Student

Electronic storage media

Minimum Instructional Facilities

1) Current version of a web enabled host
2) Computer lab with configurable hard drives installed with appropriate software, or a virtualized lab environment using either VMWare or Virtual PC/Server software that is accessible via the campus network or the Internet
3) Course management system

Method of Instruction

1) Online Computer-based reading assignments
2) Lecture and demonstration in a traditional classroom or via electronic means
3) Hands-on practice in either a dedicated or a virtual lab environment
4) Topical discussion of current operating system trends and issues

Out-of-Class Assignments

1) Complete Study Guides provided covering major topics.

2) Utilizing virtual machines configured with windows and windows server operating systems:
    a. Configure specific computer security functions and/or subsystems.
    b. Troubleshoot/analyze imposed security problems, investigate potential alternatives, and implement corrective action to achieve a determined result.
3) Complete and pass section quizzes and course final exam.
4) Read and analyze instructor assigned case studies; post analysis and comments to the class discussion board.
5) Respond to other students' analysis and comments on the class discussion board.

Texts and References

1) Recommended (representative example): Emmett Dulaney, CompTIA Security+ Study Guide SY0-401 6th edition, John Wiley & Sons, Inc., ISBN-13: 978-1-118-87507-0
2) Supplemental:
    a. CompTIA Video presentations by instructor Brian Ferrill, PACE-IT "Funded by the Department of Labor, Employment and Training Administration, Grant #TC-23745-12-60-A-53" published Oct 6, 2015. License: Creative Commons Attribution license (reuse allowed)
    b. IT Security Essentials. National Information Security and Geospatial Technologies Consortium (NISGTC) Security+, Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah. Licensed under the Creative Commons Attribution 3.0 Unported License.
    c. NISGTC Security+ V3 Labs, as distributed by The Center for Systems Security and Information Assurance (CSSIA) in partnership with the Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law these labs and future derivatives of these works. Development of these labs is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah. This work is licensed under the Creative Commons Attribution 3.0 Unported License.

Exit Skills

Students having successfully completed this course exit with the following skills, competencies and/or knowledge:

1) Identify major types of attack and malicious code.
2) Identify network security vulnerabilities.
3) Conduct a small security assessment, develop a security policy, design a secure network topology.
4) Configure security software, protocols, encryption, remote access technologies, authentication and authorization services, intrusion detection services, and equipment.

Student Learning Outcomes

Upon successful completion of this course and given a computer troubleshooting or configuration scenario, students will be able to:

1) Define network security, network topologies, security threat trends, goals of network security, and factors in a comprehensive secure network strategy.
2) Describe in detail authentication with strong passwords, Kerberos, CHAP digital certificates, tokens and biometrics.
3) 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.

4) 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.
5) Configure server, client and network security software, protocols, encryption, remote access technologies, authentication and authorization services, intrusion detection services, and equipment.
6) 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.