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 209 – CISCO CYBEROPS

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description
Designed for students seeking career-oriented, entry-level security specialist skills. Provides the technical knowledge and skill experience needed to prepare for entry-level security specialist careers. The CCNA Security curriculum blends classroom hands-on experience using Cisco routers, switches, ASAs and an online e-learning solution to develop an in-depth understanding of network security principles and security tools such as: protocol sniffers/analyzers, TCP/IP and common desktop utilities; Cisco IOS-based network security, administrative access security and Intrusion Prevention System (IPS); Cisco ASA Firewalls; AAA; and VPNs. Preparation for the Implementing Cisco Network Security (IINS) certification exam (210-260 IINS), leading to the CCNA CyberOps certification.

Prerequisite
"C" grade or higher or "Pass" in CIS 202 or equivalent or successful completion of the current version of CCNA1, and 2 at another Cisco Networking Academy or possess a current CCNA or CCENT certification

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) CCENT certification-level networking concepts and skills.
2) Design, construct and configure a basic WAN/LAN consisting of switches, routers, and workstations.
3) Restore Cisco router and switch IOS and configuration files from a TFTP server and recover a router authentication password using ROMmon.
4) Configure essential router security requirements using the Command Line Interface and a Cisco GUI Configuration Tool.
5) Configure essential switch security requirements using the Command Line Interface.
6) Configure and apply basic Standard, Access Control Lists to a router using CLI.

Course Content
1) Modern Network Security Threats
2) Authentication, Authorization and Accounting
3) Implementing Firewall Technologies
4) Implementing Intrusion Prevention
5) Securing the Local Area Network
6) Cryptographic Systems
7) Implementing Virtual Private Networks (VPNs)
8) Implementing Cisco the Adaptive Security Appliance (ASA)
9) Advanced Cisco Adaptive Security Appliance
10) Managing a Secure Network

Course Objectives
Students will be able to:
1) Describe Modern Network Security Threats
2) Implement AAA on Cisco routers
3) Implement firewall technologies to secure network perimeter.

4) Implement IPS to mitigate attacks on networks.
5) Secure endpoints and mitigate common Layer 2 attacks.
6) Secure communications to ensure integrity, authenticity and confidentiality.
7) Implement secure Virtual Private Networks.
8) Implement an ASA firewall configuration using the CLI.
9) Implement an ASA firewall configuration and VPNs using ASDM
10) Test network security and create a technical security policy.

Method of Evaluation
A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in 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 Network Security technologies, functions and characteristics, and analyze a scenario and choose the alternatives and troubleshooting options.
2) Scenario-based lab activities that measure students' ability to configure security functions, troubleshoot/analyze imposed system problems, investigate potential alternatives, and implement corrective action to achieve a determined result.
3) Practical application-based examinations that measure students' ability to evaluate a scenario-based Router/Switch /ASA network topology; analyze the topology and determine security configuration requirements/problems; configure routers, switches and ASA using the Cisco IOS CLI and/or GUI-Based configuration tools to achieve the correct requirements of the scenario.

Special Materials Required of Student
Electronic storage media

Minimum Instructional Facilities
Computers with Internet browser, Internet connectivity, and software; network connection not connected to school academic resources; 19 inch equipment racks populated with cross-connect patch panels, Cisco Access routers, switches, and ASAs, access servers; interconnecting CAT 5E and serial cabling; whiteboards; teacher desk and chair; student desks and chairs; lab desks with computers not connected to the school academic network resources; overhead computer projection system and projection screen, printer; computer server; storage cabinets.

Method of Instruction
1) Lecture and demonstration
2) Hands-on practice using the laboratory routers, switches, patch panels, access servers, computers, and virtualized PCs

Out-of-Class Assignments
May include the following:
1) Reading assignments
2) Technical skill labs using NetLabs
3) Technical skill labs using laboratory routers, switches, patch panels, access servers, computers, and virtualized PCs
4) Tests and quizzes

Texts and References
1) Required (representative example):
   a. No Textbook Required
2) Course content is provided online at www.netacad.com
   Supplemental (reference texts):

a. CCNA Security 210-260 Official Cert Guide 1st Edition; by Omar Santos (Author), John Stuppi (Author); Hardcover: 608 pages; Cisco Press; 1 edition (September 11, 2015); English; ISBN-10: 1587205661; ISBN-13: 978-1587205668
b. CCNA Security Portable Command Guide (2nd Edition) 2nd Edition; by Bob Vachon (Author); Paperback: 368 pages; Cisco Press; 2 edition (March 28, 2016); English; ISBN-10: 1587205750; ISBN-13: 978-1587205750

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 Cisco equipment.

Student Learning Outcomes

Upon successful completion of this course, students will be able to:

1) Successfully configure a defense-in-depth instructor-defined secure router/switch/ASA-based network scenario by configuring the following Security features as prescribed in the scenario: secure Router, Switch, and ASA Administrative Access; Zone-Based Policy Firewall and Intrusion Prevention System on routers; Layer-2 Switch security; ASA Firewall, and an SSL VPN.