SAN DIEGO COMMUNITY COLLEGE DISTRICT
CONTINUING EDUCATION
COURSE OUTLINE

**SECTION I**

SUBJECT AREA AND COURSE NUMBER

COMP 606

| COURSE TITLE | ALTERNATE TITLE |
|---|---|
| CISCO NETWORK SECURITY 1 | INTRO TO NETWORK SECURITY |

TYPE COURSE

NON-FEE VOCATIONAL

CATALOG COURSE DESCRIPTION

This course in Network Security focuses on an overall security process with emphasis on practical skills in security policy design and management, security technologies including, firewall and secure router design, installation, configuration and maintenance. The course also covers authentication, authorization and accounting services (AAA) as well as intrusion detection (IDS) using secure network devices. (FT)

| LECTURE HOURS | LABORATORY HOURS |
|---|---|
| 40 | 80 |

ADVISORIES

COMP 603 or equivalent

RECOMMENDED SKILL LEVEL

Possess a 10th grade reading level; the ability to communicate effectively in the English language; the knowledge of mathematical concepts at the 10th grade level and advanced computer literacy.

INSTITUTIONAL STUDENT LEARNING OUTCOMES

1. Social Responsibility
   SDCE students demonstrate interpersonal skills by learning and working cooperatively in a diverse environment.
2. Effective Communication
   SDCE students demonstrate effective communication skills.

INSTITUTIONAL STUDENT LEARNING OUTCOMES (CONTINUED)

3. Critical Thinking
   SDCE students critically process information, make decisions, and solve problems independently or cooperatively.
4. Personal and Professional Development
   SDCE students pursue short term and life-long learning goals, mastering necessary skills and using resource management and self-advocacy skills to cope with changing situations in their lives.

COURSE GOALS

Provide instruction in best practices of network security policy and management techniques. This course will prepare students to understand and identify vulnerabilities and threats as it applies to network security including terminology and acronyms. Students will learn to install, configure and secure switches, routers and firewalls with emphasis on AAA, IDS and related secure network technologies.

COURSE OBJECTIVES

Upon successful completion of this course, students will demonstrate knowledge of the security process and apply industry network security best practices including, problem solving, critical thinking ability, written and oral communication, mathematical ability and the following skills and knowledge:

1. Introduction to Vulnerabilities, Threats and Attacks
2. Security Planning and Policy – best practices
3. Installation, Configuration, and Monitoring of security devices
4. Introduction to Trust and Identity Technologies
5. Secure Access Control Services
6. Configure Trust and Identity at Layer 2 and 3
7. Configure Filtering on Firewall, Router and Switch Security Appliances
8. Emerging trend and best practices

## SECTION II

COURSE CONTENT AND SCOPE

1. Vulnerabilities, Threats, and Attacks
   - 1.1 Introduction to Network Security
     - 1.1.1 The need for network security
     - 1.1.2 Identifying potential risks to network security
     - 1.1.3 Open versus closed security models
   - 1.2 Introduction to Vulnerabilities, Threats, and Attacks
     - 1.2.1 Vulnerabilities and Malicious codes
     - 1.2.2 Threats
     - 1.2.3 Attacks, including common attack examples

COURSE CONTENT AND SCOPE (CONTINUED)

- 1.3 Vulnerability Analysis
  - 1.3.1 Policy review
  - 1.3.2 Network vs. Host analysis
  - 1.3.4 Analysis tools
2. Security Planning and Policy
   - 2.1 Discussing Network Security
     - 2.1.1 The security wheel
     - 2.1.2 Network security policy
   - 2.2 Endpoint Protection and Management
     - 2.2.1 Host and server based security components and technologies
   - 2.3 Network Protection and Management
     - 2.3.1 Network based security components and technologies
     - 2.3.2 Network security management
   - 2.4 Security Architecture
     - 2.4.1 The Intelligent, Self-Defending Networks
     - 2.4.2 Integrated security
     - 2.4.3 Plan, Design, Implement, Operate, Optimize (PDIOO)
   - 2.5 Basic Router Security
     - 2.5.1 Control access to network devices
     - 2.5.2 Remote configuration using SSH (Secure Shell)
     - 2.5.3 Router passwords
     - 2.5.4 Router privileges and accounts
     - 2.5.5 IOS (Internet Operating System) network services
     - 2.5.6 Routing, proxy ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol)
     - 2.5.7 Routing protocol authentication and update filtering
     - 2.5.8 NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), router name, DNS (Domain Name System)
3. Security Devices
   - 3.1 Device Options
     - 3.1.1 Appliance-based, server-based, and integrated firewalls
   - 3.2 Security Management Software
   - 3.3 Introduction to Security Appliances
   - 3.4. Firewall monitoring
     - 3.4.1 Time setting and NTP support
     - 3.4.2 SNMP and Syslog configuration
   - 3.5 Security Appliance Translations and Connections
     - 3.5.1 Transport protocols
     - 3.5.2 Network address translation (NAT)
     - 3.5.3 Port address translation (PAT)
     - 3.5.4 The static command
     - 3.5.5 Other related technologies
   - 3.6 Manage a Security Appliance with Adaptive Security Device Software
   - 3.7 Security Appliance Routing Capabilities
     - 3.7.1 Virtual LANs (Local Area Networks)
     - 3.7.2 Static and RIP (Routing Information Protocol) dynamic routing

COURSE CONTENT AND SCOPE (CONTINUED)

- 3.7.3 OSPF (Open Shortest Path First)
- 3.7.4 Multicast routing

4. Trust and Identity Technology
   - 4.1 Authentication, Authorization, and Accounting (AAA)
     - 4.1.1 TACACS+ (Terminal Access Controller Access Control System)
     - 4.1.2 RADIUS (Remote Authentication Dial-In User Service)
     - 4.1.3 Comparing TACACS+ and RADIUS
   - 4.2 Authentication Technologies
     - 4.2.1 Static passwords
     - 4.2.2 One-time passwords and token cards
     - 4.2.3 Digital certificates
     - 4.2.4 Biometrics
   - 4.3 Identity Based Networking Services (IBNS)
     - 4.3.1 Introduction to IBNS
     - 4.3.2 Introduction to 802.1x
     - 4.3.3 Wired and wireless implementations
   - 4.4 Network Admission Control (NAC)
     - 4.4.1 NAC components
     - 4.4.2 NAC phases
     - 4.4.3 NAC operation
     - 4.4.4 NAC vendor participation
5. Secure Access Control Server
   - 5.1 Secure Access Control Server (CSACS) for Windows
   - 5.2 Configuring RADIUS and TACACS+ with CSACS
     - 5.2.1 Installation steps
     - 5.2.2 Administering Secure ACS for Windows
     - 5.2.3 Troubleshooting
     - 5.2.4 Enabling and Verifying TACACS+
     - 5.2.5 Configuring RADIUS
6. Configure Trust and Identity at Layer 3
   - 6.1 Firewall Authentication Proxy
     - 6.1.1 AAA server and device configuration
     - 6.1.2 Allow AAA traffic to the router
     - 6.1.3 Authentication proxy configuration
   - 6.2 Introduction to Security Appliance AAA Features
     - 6.2.1 Security Appliance authentication, authorization and accounting
   - 6.3 Configure AAA on the Security Appliance
     - 6.3.1 Troubleshooting the AAA configuration
7. Configure Trust and Identity at Layer 2
   - 7.1 Identity-Based Networking Services (IBNS)
     - 7.1.1 IBNS overview
     - 7.1.2 IEEE 802.1x

COURSE CONTENT AND SCOPE (CONTINUED)

- 7.2 Configuring 802.1x Port-Based Authentication
  - 7.2.1 802.1x port-based authentication configuration tasks
  - 7.2.2 Enabling 802.1x authentication
8. Configure Filtering on a Router
   - 8.1 Filtering Technologies
     - 8.1.1 Packet filtering
     - 8.1.2 Stateful filtering
     - 8.1.3 URL filtering
   - 8.2 Firewall Context-Based Access Control
     - 8.2.1 How CBAC works
   - 8.3 Configure Firewall Context-Based Access Control
9. Configure Filtering on a Security Appliance
   - 9.1 Configure ACLs (Access Control Lists) and Content Filters
     - 9.1.1 Security Appliance ACLs
     - 9.1.2 The icmp (internet control message protocol) command
     - 9.1.3 (NAT) 0 ACLs
   - 9.2 Object Grouping
     - 9.2.1 Overview of object grouping
   - 9.3 Configure a Security Appliance Modular Policy
     - 9.3.1 Modular policy overview
   - 9.4 Configure Advanced Protocol Inspection
     - 9.4.1 Introduction to advanced protocol inspection
     - 9.4.2 Default traffic inspection and port numbers
10. Configure Filtering on a Switch
    - 10.1 Introduction to Layer 2 Attacks
      - 10.1.1 Types of attacks
    - 10.2 MAC (Media Address Control) Address, ARP (Address Resolution Protocol), and DHCP (Dynamic Host Control Protocol) Vulnerabilities
      - 10.2.1 CAM (Content Addressable Memory) table overflow attack
      - 10.2.2 Mitigating the CAM table overflow attack
      - 10.2.3 MAC spoofing – man in the middle attacks
    - 10.3 VLAN Vulnerabilities
      - 10.3.1 VLAN hopping attacks
      - 10.3.2 Mitigating VLAN hopping attacks
    - 10.4 Spanning-Tree Protocol Vulnerabilities
      - 10.4.1 Spanning-Tree Protocol vulnerabilities

APPROPRIATE READINGS

Appropriate readings may include, but are not limited to, periodicals, magazines, instructor-written materials, manuals, instructor selected URLs, and publications related to network security design and theory.

## WRITING ASSIGNMENTS

Appropriate writing assignments may include, but are not limited to, preparing text for an assigned project, document all laboratory and project work and completing all written assigned reports.

## OUTSIDE ASSIGNMENTS

Outside assignments may include, but are not limited to, reading texts and reference resources; research as needed to complete projects; and organizing and preparing written answers to assigned questions.

## APPROPRIATE ASSIGNMENTS THAT DEMONSTRATE CRITICAL THINKING

Assignments that demonstrate critical thinking may include, but are not limited to, analysis and evaluation of assigned text and reference resources, and the utilization of this analysis in classroom discussions, writing assignments, and in performing laboratory activities. Students must use appropriate methods and resources to complete laboratory assignments.

## EVALUATION

Evaluation will be based on multiple measures of performance. Assessments will measure development of independent critical thinking skills and will include measuring students' ability to:

1. Perform the manipulative skills of the craft, as required.
2. Apply theory to practical hands on lab assignments.
3. Perform in a variety of activities and assignments.
4. Successfully complete the final exam.
5. Complete written, oral, and practical examinations.
6. Contribute to class discussions.
7. Maintain attendance per current policy.
8. Demonstrate troubleshooting skills.
9. Demonstrate subject mastery by collaborating with team members to complete a real world case study

Satisfactory completion of the course requires completion of a culminating activity, which may include, but not limited to, one of the following:

1. Skills based assessment.
2. Classroom presentation.
3. Practical Lab projects, which include practical demonstrations securing network devices like switches and router, design and implementation of corporate security policies, best practices for intrusion mitigation, configuring AAA, IEEE 802.1x, RADIUS, TACACS and other secure access technologies.

METHOD OF INSTRUCTION

Methods of instruction may include, but are not limited to, lecture, self-paced lab, demonstration, individualized study, use of multimedia presentations, group/team work, tutorials, and other unique instruction requirements, such as, outside assignments, real or virtual field trips, and guided student job assignments.

This course, or sections of this course, may be offered through distance education.

TEXTS AND SUPPLIES

*Network Security 1 and 2 Companion Guide (Cisco Networking Academy Program)*
Cisco Press, current edition

Web resources:
www.cisco.com
www.cisco.netacad.net
www.nsca-cc.org
www.auditmypc.com

Supplies: personal storage

PREPARED BY Maria Reyes & Don Aragon DATE December 5, 2007

REVISED BY Instructional Services/SLO's Added DATE May 30, 2013

REVISED BY Don Aragon & Richard Gholson DATE May 08, 2015

REVISED BY Don Aragon & Richard Gholson DATE May 08, 2015

REVISED BY Don Aragon & Richard Gholson DATE May 6, 2020

Instructors must meet all requirements stated in Policy 3100 (Student Rights, Responsibilities and Administrative Due Process), and the Attendance Policy set forth in the Continuing Education Catalog.

REFERENCES:

San Diego Community College District Policy 3100
California Community Colleges, Title 5, Section 55002

Continuing Education Catalog