SAN DIEGO COMMUNITY COLLEGE DISTRICT
CONTINUING EDUCATION
COURSE OUTLINE

SECTION I

SUBJECT AREA AND COURSE NUMBER

COMP 609

COURSE TITLE

NETWORK SECURITY BASICS

TYPE COURSE

NON-FEE VOCATIONAL

CATALOG COURSE DESCRIPTION

This course provides the foundation and basic skills needed in computer and network security. Topics include identifying security risks, risk mitigation strategies, forensic procedures, incident response procedures and cryptography. Students will learn investigative techniques, types of threats, and application of security controls to maintain confidentiality, data integrity, and availability. Emphasis will be placed on security best practices and applying applicable policies, laws, and regulations. (FT)

LECTURE/LABORATORY HOURS

120

ADVISORIES

COMP 608 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

1. Students will learn the concepts and techniques of computer and network security.
2. Students will learn how to apply and secure configurations on network devices.
3. Students will gain experience with security and risk management best practices.
4. Students will gain knowledge of security risks in applications, hosts and network infrastructure.
5. Students will learn about the techniques and best practices for analyzing and responding to security incidents.
6. Students will gain knowledge of appropriate threat response strategies for the different types of attacks.
7. Students will learn how to apply authentication, authorization, and access control to secure data.
8. Students will gain knowledge of appropriate cryptographic concepts and methods to secure data.

COURSE OBJECTIVES

Upon successful completion of this course, the students will be able to:
1. Explain and implement configurations on network devices that comply with security best practices.
2. Describe risk management best practices including applicable laws, policies and regulations.
3. Analyze network design elements for security risks.
4. Select the appropriate tools and techniques to discover and mitigate security risks to computer systems.
5. Demonstrate and apply appropriate forensic and security incident response procedures.
6. Explain which types of malware are used for the different types of attacks and the appropriate measures to apply to mitigate an attack.
7. Select and apply the appropriate authentication, authorization and access control measures to ensure data security.
8. Explain, compare and utilize appropriate cryptographic concepts and methods.

SECTION II

COURSE CONTENT AND SCOPE

1. Network Security
    1.1. Device configuration parameters
        1.1.1. Firewalls
        1.1.2. Routers
        1.1.3. Switches
        1.1.4. Load balancers
        1.1.5. Other current devices
    1.2. Security policies
        1.2.1. Rule-based management
        1.2.2. Secure network device configuration
        1.2.3. Information security policy
    1.3. Network design elements and components
        1.3.1. Demilitarized zone (DMZ)
        1.3.2. IPv4 and IPv6 subnets
        1.3.3. Layer 2 and layer 3 security components
        1.3.4. Remote access
        1.3.5. Emerging network technologies
    1.4. Common protocols and services
        1.4.1. TCP/IP (Transport Control Protocol/Internet Protocol) protocols
        1.4.2. Common TCP/IP Ports and other ports required for a secure environment
    1.5. Wireless networking security
        1.5.1. Encryption protocols
        1.5.2. Best practices related to security concerns
2. Compliance and Operational Security
    2.1. Risk related concepts
        2.1.1. Technical, management/financial, and operational
        2.1.2. False positives/false negatives
        2.1.3. Organizational, operational and other policies in reducing risk
    2.2. System Integration
        2.2.1. On-boarding/off-boarding business partners
        2.2.2. Social media networks and/or other applications
        2.2.3. Interoperability agreements
    2.3. Risk mitigation strategies
        2.3.1. Change management
        2.3.2. Incident management
        2.3.3. User rights and permissions reviews
        2.3.4. Audits
        2.3.5. Policy and procedure enforcement
        2.3.6. Data loss prevention
    2.4. Forensic procedures
        2.4.1. Capture system image
        2.4.2. Network traffic and logs
        2.4.3. Chain of custody
        2.4.4. Data analysis

COURSE CONTENT AND SCOPE (CONTINUED)

- 2.5. Incident response procedures
  - 2.5.1. Preparation for incidence response including pre-planning
  - 2.5.2. Incident identification
  - 2.5.3. Escalation and notification
  - 2.5.4. Mitigation implementation
  - 2.5.5. Incident response review
- 2.6. Security related awareness and training
  - 2.6.1. Security policy training and procedures
  - 2.6.2. Role-based training
  - 2.6.3. Information classification
  - 2.6.4. Legal compliance, best practices and standards
  - 2.6.5. Emerging threats, trends, and alerts
- 2.7. Physical security and environmental controls
  - 2.7.1. Environmental controls
  - 2.7.2. Physical security
  - 2.7.3. Control types
- 2.8. Security goals
  - 2.8.1. Confidentiality, encryption, and Integrity
  - 2.8.2. Access controls for physical security
  - 2.8.3. Risk management

3. Threats and Vulnerabilities
   - 3.1. Types of malware
   - 3.2. Types of attacks
   - 3.3. Social engineering attacks
     - 3.3.1. Shoulder surfing
     - 3.3.2. Dumpster diving
     - 3.3.3. Current social engineering attacks
   - 3.4. Wireless attacks
   - 3.5. Types of application attacks
   - 3.6. Appropriate type of mitigation and deterrence
     - 3.6.1. Monitoring system logs
     - 3.6.2. Hardening
     - 3.6.3. Current mitigation technologies and techniques
   - 3.7. Discovery tools and techniques
     - 3.7.1. Security assessment tools
     - 3.7.2. Risk calculations
     - 3.7.3. Assessment techniques
   - 3.8. Penetration testing versus vulnerability scanning
4. Application, Data and Host Security
   - 4.1. Application security controls and techniques
   - 4.2. Mobile security concepts and technologies
     - 4.2.1. Device security
   - 4.3. Controls to ensure data security
     - 4.3.1. Cloud storage
     - 4.3.2. Storage Area Network (SAN)
     - 4.3.3. Current controls methods
   - 4.4. Risk mitigation in static environments

COURSE CONTENT AND SCOPE (CONTINUED)

5. Access Control and Identity Management
    5.1. Function and purpose of authentication services
    5.2. Identification vs. authentication vs. authorization
        5.2.1. Authorization
        5.2.2. Authentication
        5.2.3. Authentication factors
        5.2.4. Identification
        5.2.5. Federation
        5.2.6. Transitive trust/authentication
    5.3. Account management best practices
6. Cryptography
    6.1. General cryptography concepts
        6.1.1. Symmetric vs. asymmetric
        6.1.2. Session keys
        6.1.3. Transport encryption
        6.1.4. Non-repudiation
        6.1.5. Hashing
        6.1.6. Digital signatures
    6.2. Cryptographic methods
        6.2.1. Algorithms
        6.2.2. Protocols
        6.2.3. Transport encryption
    6.3. PKI (Public Key Infrastructure) and certificate management
        6.3.1. Certificate authorities and digital certificates
        6.3.2. PKI
        6.3.3. Public and private keys
        6.3.4. Trust models

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.

WRITING ASSIGNMENTS

Appropriate writing assignments may include, but are not limited to, preparing text for an assigned project, documenting laboratories and project work, and completing 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 which 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

A student's grade will be based on multiple measures of performance and will include evaluation of student's ability to:

1. Apply theory to practical hands on lab assignments.
2. Perform in a variety of activities and assignments.
3. Complete written and practical examinations.
4. Successfully complete final exam.
5. Contribute to class and group discussions.
6. Maintain attendance and punctuality per current policy.
7. Demonstrate troubleshooting skills
8. Demonstrate ability to work independently and as a team member.

Upon successful completion of each course in the program, a Certificate of Course Completion will be issued. Upon successful completion of all courses included in the program, a Certificate of Program Completion will be issued.

METHOD OF INSTRUCTION

Methods of instruction may include, but are not limited to, lectures, discussion, hands-on demonstrations, computer-assisted instruction, laboratory assignments and field trips. This course, or sections of this course, may be offered through distance education.

TEXTS AND SUPPLIES

CompTIA Security+ Study Guide, Dulaney and Easttom, Sybex, current edition
Web resources: comptia.org
Supplies: Journal (composition book), USB Drive or other storage media

PREPARED BY: Don Aragon DATE: March 27, 2015

REVISED BY: _____ DATE: _____

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