SAN DIEGO COMMUNITY COLLEGE DISTRICT
CONTINUING EDUCATION
COURSE OUTLINE

SECTION I

SUBJECT AREA AND COURSE NUMBER

COMP 657

COURSE TITLE

CYBERSECURITY ARCHITECTURE

TYPE COURSE

NON-FEE VOCATIONAL

CATALOG COURSE DESCRIPTION

This course covers cybersecurity architecture and tools. Students will use tools and guidelines to build a set of security policies and procedures. Students will also design a layered security architecture and analyze it for flaws. Topics include security frameworks, policies, and controls used for remediation. Students use industry standards for software security. The review, selection, and assembly of tools for performing threat and incident management will also be covered. (FT)

LECTURE/LABORATORY HOURS

45

ADVISORIES

COMP 655 Cyber Threat And Vulnerability; and
COMP 656 Intro Cyber Incident Response or equivalents

RECOMMENDED SKILL LEVEL

Possess a 12th grade reading level; ability to communicate effectively in the English language; knowledge of math concepts at the 8th grade level and 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. Gain an understanding of a well-designed cybersecurity architecture.
2. Learn about the information security framework, including policies, controls, and procedures.
3. Learn how to use data to make recommendations for remediation of identity and access management issues.
4. Learn about the common exploits used to compromise identity.
5. Explore data analytics and how it is used to determine appropriate compensating controls.
6. Learn how to implement defense-in-depth to secure networks and systems.
7. Learn how to apply secure coding best practices as a part of the Software Development Life Cycle.
8. Explore the purpose and use of common cybersecurity tools and technologies.

COURSE OBJECTIVES

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

1. Describe the importance of a well-designed cybersecurity architecture.
2. Explain the relationship between an information security policy framework, and common security policies, standards, procedures, and guidelines.
3. Use data to recommend remediation of security issues related to identity and access management.
4. Explain the key components associated with security architecture and network design principles.
5. Make recommendations to implement compensating controls as part of a security architecture review.
6. Describe the processes associated with application security testing.
7. Apply application security best practices while participating in the software development life cycle.
8. Compare and contrast the purpose and reason for using common cybersecurity tools and technologies.

SECTION II

COURSE CONTENT AND SCOPE

1. Regulatory Compliance Considerations
   1.1. Frameworks

COURSE CONTENT AND SCOPE (CONTINUED)

1.1.1. NIST (National Institute of Standards and Technology)
1.1.2. ISO (International Standards Organization)
1.1.3. COBIT (Control Objectives for Information and Related Technologies)
1.1.4. SABSA (Sherwood Applied Business Security Architecture)
1.1.5. TOGAF (The Open Group Architecture Forum)
1.1.6. ITIL (Information Technology Infrastructure Library)
1.2. Policies
1.2.1. Password
1.2.2. Acceptable use
1.2.3. Data ownership
1.2.4. Data retention
1.2.5. Account management
1.2.6. Data classification
1.3. Controls
1.3.1. Criteria for selection
1.3.2. Organizationally defined parameters
1.3.3. Physical
1.3.4. Logical
1.3.5. Administrative
1.4. Procedures
1.4.1. Continuous monitoring
1.4.2. Evidence production
1.4.3. Patching
1.4.4. Compensating control development
1.4.5. Control testing procedures
1.4.6. Manage exceptions
1.4.7. Remediation plans
1.5. Verifications and quality control
1.5.1. Audits
1.5.2. Evaluations
1.5.3. Assessments
1.5.4. Maturity model
1.5.5. Certification
2. Remediation Recommendations for Identity and Access Management Security Issues
2.1. Context-based authentication issues
2.1.1. Time
2.1.2. Location
2.1.3. Frequency
2.1.4. Behavioral
2.2. Identities issues
2.2.1. Personnel
2.2.2. Endpoints
2.2.3. Servers
2.2.4. Services
2.2.5. Roles
2.2.6. Applications

COURSE CONTENT AND SCOPE (CONTINUED)

- 2.3. Identity repositories issues
  - 2.3.1. Directory services
  - 2.3.2. TACACS+ (Terminal Access Controller Access Control System)
  - 2.3.3. RADIUS (Remote Authentication Dial-In User Service)
- 2.4. Federation and single sign-on issues
  - 2.4.1. Manual and automatic provisioning and de-provisioning
  - 2.4.2. Self-service password reset
- 2.5. Exploits
  - 2.5.1. Impersonation
  - 2.5.2. Man-in-the-middle
  - 2.5.3. Session hijack
  - 2.5.4. Cross-site scripting
  - 2.5.5. Privilege escalation
  - 2.5.6. Rootkit

3. Security Architecture Review and Recommendations

- 3.1. Security data analytics
  - 3.1.1. Data aggregation and correlation
  - 3.1.2. Trend analysis
  - 3.1.3. Historical analysis
- 3.2. Manual log review
  - 3.2.1. Firewall
  - 3.2.2. Syslog
  - 3.2.3. Authentication
  - 3.2.4. Event
- 3.3. Defense in depth
- 3.4. Personnel Security
  - 3.4.1. Training
  - 3.4.2. Dual control
  - 3.4.3. Separation of duties
  - 3.4.4. Third party consultants
  - 3.4.5. Cross training
  - 3.4.6. Mandatory vacation
  - 3.4.7. Succession planning
- 3.5. Processes
  - 3.5.1. Continual improvement
  - 3.5.2. Scheduled reviews
  - 3.5.3. Retirement of processes
- 3.6. Technologies
  - 3.6.1. Automated reporting
  - 3.6.2. Security appliances
  - 3.6.3. Security suites
  - 3.6.4. Outsourcing
  - 3.6.5. Security as a Service
  - 3.6.6. Cryptography
- 3.7. Network design
- 3.8. Network segmentation

COURSE CONTENT AND SCOPE (CONTINUED)

4. SDLC (Software Development Life Cycle) and Application Security Best Practices
   - 4.1. Software development best practices
     - 4.1.1. Security requirements definition
     - 4.1.2. Manual peer reviews
     - 4.1.3. User acceptance testing
     - 4.1.4. Stress test application
     - 4.1.5. Security regression testing
     - 4.1.6. Input validation
   - 4.2. Security testing phases
     - 4.2.1. Static code analysis
     - 4.2.2. Web app vulnerability scanning
     - 4.2.3. Fuzzing
     - 4.2.4. Interception proxy to crawl application
   - 4.3. Secure coding best practices
     - 4.3.1. OWASP (Open Web Application Security Project)
     - 4.3.2. SANS (System Administration, Networking, and Security Institute)
     - 4.3.3. Center for Internet Security
     - 4.3.4. System design recommendations
     - 4.3.5. Benchmarks
5. Cybersecurity Tools and Technologies
   - 5.1. Preventative
     - 5.1.1. IPS (intrusion prevention system)
     - 5.1.2. HIPS (host intrusion prevention system)
     - 5.1.3. Firewall
     - 5.1.4. Antivirus
     - 5.1.5. Anti-malware
     - 5.1.6. EMET (Enhanced Mitigation Experience Toolkit)
     - 5.1.7. Web proxy
     - 5.1.8. WAF (web application firewall)
   - 5.2. Collective
     - 5.2.1. SIEM (security information and event management)
     - 5.2.2. Network scanning
     - 5.2.3. Vulnerability scanning
     - 5.2.4. Packet capture
     - 5.2.5. Command line
     - 5.2.6. IP (internet protocol) utilities
     - 5.2.7. IDS (intrusion detection system)
     - 5.2.8. HIDS (host intrusion detection system)
   - 5.3. Analytical
     - 5.3.1. Vulnerability scanning
     - 5.3.2. Monitoring tools
     - 5.3.3. Interception proxy
   - 5.4. Exploit
     - 5.4.1. Interception proxy
     - 5.4.2. Exploit framework
     - 5.4.3. Fuzzers

COURSE CONTENT AND SCOPE (CONTINUED)

5.5. Forensics
- 5.5.1. Forensic suites
- 5.5.2. Hashing
- 5.5.3. Password cracking
- 5.5.4. Imaging

APPROPRIATE READINGS

Readings may include, but are not limited to, textbooks, manuals, periodicals, instructor-written materials, and websites. Reading subject matter would be related to the information security framework, remediation procedures and controls, and application security best practices.

WRITING ASSIGNMENTS

Appropriate writing assignments may include, but are not limited to, preparing text for an assigned project, documenting all laboratories and project work, and completing all written assigned reports. A report may include preparing a written recommendation describing how to handle a privilege escalation issue.

OUTSIDE ASSIGNMENTS

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

APPROPRIATE ASSIGNMENTS THAT DEMONSTRATE CRITICAL THINKING

Assignments which demonstrate critical thinking may include analysis and evaluation of assigned text and reference resources. Such analysis may be used in classroom discussions, as well as completing lab activities such as performing vulnerability scans. An appropriate assignment may include designing a layered security architecture and analyzing it for flaws. Students must select appropriate methods and resources needed 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. Perform in a variety of activities and assignments related to the course objectives.
2. Complete written and practical examinations.
3. Contribute to class and group discussions.
4. Maintain attendance and punctuality per current policy.
5. Demonstrate ability to work independently and as a team member.

EVALUATION (CONTINUED)

6. Demonstrate troubleshooting skills.

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, self-paced lab, demonstrations, individualized study, use of audio-visual aids, group/team work, tutorials, outside assignments, guest lectures, field trips, and guided student job assignments. This course, or sections of this course, may be offered through distance education.

TEXTS AND SUPPLIES

CompTIA Cybersecurity Analyst (CSA+) Study Guide: Exam CS0-001, Michael J. Chapple, David Seidl, Sybex, current edition
CompTIA Cybersecurity Analyst (CSA+) Cert Guide (Certification Guide), Troy McMillan, Pearson, current edition
CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001), Fernando Maymi, Brent Chapman, McGraw Hill, current edition

Web Resources:
ITPRO.TV, https://itpro.tv/course-library/cybersecurity-analyst-csa/overview70770/ ;
CompTIA Marketplace, https://www.comptiastore.com/CompTIA-Cybersecurity-Analyst-CSA-eBook-Labs-p/pl720ebk.htm;
CYBRARY, https://www.cybrary.it/catalog/practice_labs/comptia-cybersecurity-analyst-csa

Supplies: Journal (composition book), USB Drive or other storage media

PREPARED BY: Richard Gholson DATE: February 7, 2018

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