SAN DIEGO COMMUNITY COLLEGE DISTRICT
CONTINUING EDUCATION
COURSE OUTLINE

SECTION I

SUBJECT AREA AND COURSE NUMBER

COMP 655

COURSE TITLE

CYBER THREAT AND VULNERABILITY

TYPE COURSE

NON-FEE VOCATIONAL

CATALOG COURSE DESCRIPTION

This course covers cybersecurity threat and vulnerability assessment and remediation. Students employ threat assessments to select the appropriate controls to secure a network or system. Students use tools for environmental and network reconnaissance, and apply techniques to minimize their impact. Topics include reconnaissance analysis and corporate security practices. Students also design and use a vulnerability management program to identify, prioritize, and remediate organizational vulnerabilities. (FT)

LECTURE/LABORATORY HOURS

45

ADVISORIES

COMP 608 Basic Network Configuration; and
COMP 609 Network Security Basics 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 cybersecurity threats.
2. Learn about reconnaissance techniques and tools used by security threats.
3. Learn how to analyze common logs for threat management.
4. Explore penetration testing tools and how to apply them to secure a network.
5. Gain an understanding of common vulnerabilities within an organization.
6. Learn how to perform and analyze the output of a vulnerability scan.

COURSE OBJECTIVES

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

1. Describe the roles and responsibilities of cybersecurity analysts.
2. Apply environmental reconnaissance techniques using appropriate tools and processes.
3. Analyze the results of a network reconnaissance.
4. Given a network-based threat, implement or recommend the appropriate response and countermeasure.
5. Explain the purpose of practices used to secure a corporate environment.
6. Implement an information security vulnerability management process.
7. Configure vulnerability scanning tools and analyze resulting output.
8. Compare and contrast common vulnerabilities found within an organization.
9. Describe the major steps associated with a typical penetration testing process.
10. Analyze the environment and outline its vulnerability management requirements.

SECTION II

COURSE CONTENT AND SCOPE

1. Environmental Reconnaissance Techniques for Threat Management
   1.1. Procedures/common tasks
      1.1.1. Topology discovery
      1.1.2. OS (operating system) fingerprinting
      1.1.3. Service discovery
      1.1.4. Packet capture
      1.1.5. Log review
      1.1.6. Router/firewall ACLs (access control list) review

COURSE CONTENT AND SCOPE (CONTINUED)

- 1.1.7. Email harvesting
- 1.1.8. Social media profiling
- 1.1.9. Social engineering
- 1.1.10. DNS (Domain Name System) harvesting
- 1.1.11. Phishing

1.2. Variables
- 1.2.1. Wireless, wired
- 1.2.2. Virtual, physical
- 1.2.3. Internal, external
- 1.2.4. On-premises, cloud

1.3. Tools
- 1.3.1. Network mapping and statistics
- 1.3.2. Host and network scanners
- 1.3.3. Packet analyzer
- 1.3.4. IDS (intrusion detection system)
- 1.3.5. IPS (intrusion prevention system)
- 1.3.6. Firewall rules and logs
- 1.3.7. System log server
- 1.3.8. Vulnerability scanner

2. Network Reconnaissance Analysis for Threat Management

2.1. Point-in-time data analysis
- 2.1.1. Packet
- 2.1.2. Protocol
- 2.1.3. Traffic
- 2.1.4. Netflow protocol
- 2.1.5. Wireless

2.2. Data correlation and analytics
- 2.2.1. Anomalies
- 2.2.2. Trends
- 2.2.3. Availability
- 2.2.4. Heuristics
- 2.2.5. Behavioral

2.3. Data output
- 2.3.1. Packet captures
- 2.3.2. Network mapping scan results
- 2.3.3. Event, system, and firewall logs
- 2.3.4. IDS/IPS reports

2.4. Tools
- 2.4.1. SIEM (security information and event management)
- 2.4.2. Packet analyzer
- 2.4.3. IDS/IPS
- 2.4.4. Resource monitoring tool
- 2.4.5. Netflow analyzer

3. Network Threat Response and Countermeasures

3.1. Network segmentation
- 3.1.1. System isolation

COURSE CONTENT AND SCOPE (CONTINUED)

3.1.2. Jump box
3.2. Honeypots
3.3. Endpoint security
3.4. Group policies
3.5. ACLs
3.5.1. Sinkhole
3.6. Hardening
3.6.1. MAC (mandatory access control)
3.6.2. Compensating controls
3.6.3. Blocking unused ports/services
3.6.4. Patching
3.7. NAC (Network Access Control)
3.7.1. Basis by time, rule, role, and location
4. Corporate Environment Security Practices
4.1. Penetration testing rules of engagement
4.1.1. Timing
4.1.2. Scope
4.1.3. Authorization
4.1.4. Exploitation
4.1.5. Communication
4.1.6. Reporting
4.2. Reverse engineering
4.2.1. Isolation/sandboxing
4.2.2. Hardware authenticity
4.2.3. Malware fingerprinting
4.2.4. Software hashing
4.2.5. Software decomposition
4.3. Training and exercises
4.3.1. Types of teams including offense, defense, and referees
4.4. Risk evaluation
4.4.1. Technical and operational controls
4.4.2. Technical impact and likelihood
5. Vulnerability Management Process
5.1. Requirements
5.1.1. Regulatory environments
5.1.2. Corporate policy
5.1.3. Data classification
5.1.4. Asset inventory
5.2. Scan frequency
5.2.1. Risk appetite
5.2.2. Regulatory requirements
5.2.3. Technical constraints
5.2.4. Workflow
5.3. Scan tool configuration
5.3.1. Scan criteria, including sensitivity levels, scope, data types
5.3.2. Updates and plug-ins

COURSE CONTENT AND SCOPE (CONTINUED)

- 5.3.3. Permissions and access
- 5.4. Scan execution
- 5.5. Reports
  - 5.5.1. Distribution types: manual, automated
- 5.6. Remediation
  - 5.6.1. Prioritization: criticality, degree of difficulty
  - 5.6.2. Control types: communication, change
  - 5.6.3. Sandboxing, testing
  - 5.6.4. Types of inhibitors including MOUs (memorandum of understanding), SLAs (service level agreement), governance, business process interruption
- 5.7. Ongoing scanning and continuous monitoring

6. Vulnerability Scan Analytics
   - 6.1. Scan report analysis
     - 6.1.1. Review and interpretation: false positives, exceptions
     - 6.1.2. Response action prioritization
   - 6.2. Result validation and correlation
     - 6.2.1. Best practices or compliance
     - 6.2.2. Result reconciliation
     - 6.2.3. Log review
     - 6.2.4. Trends
7. Organizational Vulnerabilities
   - 7.1. Servers
   - 7.2. Endpoints
   - 7.3. Network infrastructure
   - 7.4. Network appliances
   - 7.5. Virtual Infrastructure
     - 7.5.1. Hosts
     - 7.5.2. Networks
     - 7.5.3. Management interface
   - 7.6. Mobile devices
   - 7.7. Interconnected networks
   - 7.8. VPN (virtual private network)
   - 7.9. ICS (industrial control systems)
   - 7.10. SCADA (supervisory control and data acquisition) devices

APPROPRIATE READINGS

Readings may include, but are not limited to, textbooks, manuals, periodicals, instructor-written materials, and websites. Topics should be related to cybersecurity threats and vulnerabilities, including reconnaissance techniques, vulnerability scans, and threat response.

WRITING ASSIGNMENTS

Appropriate writing assignments may include, but are not limited to, preparing text for an assigned project, documenting all laboratories and project work including the results of network and vulnerability scans, and completing all written assigned reports, such as

WRITING ASSIGNMENTS (CONTINUED)

penetration testing rules of engagement.

OUTSIDE ASSIGNMENTS

Outside assignments may include, but are not limited to, reading texts and reference resources; research as needed to complete projects, such as determining the elements of a penetration testing plan; and organizing and preparing written answers to assigned questions.

APPROPRIATE ASSIGNMENTS THAT DEMONSTRATE CRITICAL THINKING

Assignments which exhibit critical thinking may include analysis and evaluation of assigned text and reference resources, and utilizing this analysis in classroom discussions, as well as completing lab activities. An appropriate assignment includes interpreting the results of a vulnerability scan and using that to develop a remediation plan for a network.

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.
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

TEXTS AND SUPPLIES (CONTINUED)

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