CYBR C260: INTERMEDIATE INCIDENT RESPONSE

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	72 Total Hours (Lecture Hours 54; Lab Hours 18)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Students will explore incident response techniques using industry-recognized tools. Topics covered include planning and scoping a cyber incident, information gathering for vulnerability assessment, vulnerability scanning and summarization reporting, report writing and best practices, obfuscation techniques, forensic artifacts, social media forensics, memory forensics, ethics, and compliance issues. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. ADVISORY: IT C128 and CYBR C230.Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Outline an incident plan and scope for an assessment.
2. Demonstrate the use of appropriate tools and techniques to perform vulnerability scanning and locate indicators of compromise.
3. Analyze results of vulnerability scan to provide practical recommendations for management.

Course Objectives

- 1. Demonstrate an understanding of the Incident Response process, including scoping, planning, and reporting.
- 2. Describe the need for vulnerability scanning and use of indicators of compromise as applied to cyber incident handling.
- 3. Demonstrate an understanding of forensic artifacts, including social media, computer memory.
- 4. Demonstrate an understanding of law enforcement careers and emerging trends in the field of incident response.

Lecture Content

Planning Gather information on systems to be evaluated Indicators of compromise Purpose of review 1. Civil case 2. Divorce 3. Family law Role of ethics and compliance Establishing scope of the project Identify tools needed for information gathering Penetration Testing Perform vulnerability scan Commonly used tools1. Cobalt Strike2. Metasploit3. SIFT workstation4. SIEM workstation Understanding Code Obfuscation Techniques Exploit network Analyze results Collect forensic artifacts from red team activity Incident Response Topics Social media forensics Memory forensics Point of Sale (POS) Payment Systems Linux Forensics Reporting Techniques Draft management report Summarize results Provide recommendations Update risk assessment based on findings

Lab Content

Students will work with remote lab environments to complete hands-on activities. Scan network for vulnerabilities and summarize results Conduct information gathering exercises using various tools (eg. Cobalt Strike, Metasploit, SIFT workstation, SIEM) Detect obfuscation techniques Locate indicators of compromise Create a comprehensive report of evidence collected Locate forensic artifacts from red team activity Find the pivot point of an investigation Find the time anchor for an incident Social media forensics Memory forensics Linux forensics Create a comprehensive report of evidence collected throughout the process

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read about incident response techniques and planning. Read about commonly used tools used in incident response. Read about code obfuscation techniques.

Writing Assignments

Draft a report for management detailing results of vulnerability scan. Perform an update to risk assessment rating based on the work performed.

Out-of-class Assignments

Complete hands-on lab using commonly used tools to perform a vulnerability scan. Complete hands-on lab to collect forensic artifacts from red team activities.

Demonstration of Critical Thinking

Students will conduct vulnerability scan using best practices processes and procedures.

Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through completion of hands-on lab exercises using commonly used vulnerability assessment tools and document analysis performed to provide management recommendations.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Anson, S. Applied Incident Response, 1st ed. John Wiley Sons, 2020

Other Resources

1. Coastline Library 2. OER - Open Educational Resources