CYBR C132: INTRODUCTION TO ETHICAL HACKING

Item	Value
Curriculum Committee Approval Date	02/26/2021
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Formerly: CST C232B. This course is an introduction to the ethical and legal issues pertaining to network and computer security testing. Students will explore an introduction to the hacking methodology and network penetration testing using industry-recognized tools. Hands-on assignments will be used to help students develop introductory technical skills relevant to entry-level cybersecurity professionals, including demonstration of tools that can be used to gain information about a computer network, web applications, and databases. This course is intended for students with computer experience and an interest in cyber defense for private organizations. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Given a lab scenario, analyze and test for vulnerabilities using industry-recognized tools and describe the findings.
2. Given a lab scenario, apply the hacking methodology using industry-recognized tools to gain unauthorized access to a computer or networked system.
3. Given a scenario, report on ethical issues, laws, policies, and/or regulations related to appropriate computer use and network testing to address vulnerability assessment findings.

Course Objectives

- 1. Explain the hacking methodology and tools used to gain unauthorized access to computer or networked system.
- 2. Provide demonstrations to help students understand how to analyze and assess a computer or networked system to find vulnerabilities.
- 3. Explain ethical issues, laws, policies, and regulations related to appropriate computer use and network testing for security professionals.

Lecture Content

Hacker Techniques and Tools Hacking: The Next Generation TCP/IP Review Cryptographic Concepts The Hacking Methodology A Technical and Social Overview of Hacking Footprinting Tools and Techniques Port Scanning Enumeration and Computer Systems Hacking Wireless Vulnerabilities Web and Database Attacks Malware Sniffers, Session Hijacking, and Denial of Service Attacks Linux and Penetration Testing Footprinting and Social Engineering Incident Response and Defensive Techniques Incident Response Defensive Technologies Operating System Vulnerabilities Microsoft Platforms Linux Distributions Protecting Networks with Security Devices Routers Firewalls Intrusion Prevention and Detection

Lab Content

Vulnerability scanning of computer networked systems Penetration testing of computer networked systems Reconnaissance and network scanning Social engineering Web application probing Password cracking Enumeration of computer networked systems

Method(s) of Instruction

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

Instructional Techniques

Instructional techniques for this course will come in the format of face-to-face, hybrid, or online formats. All of these formats will incorporate instructional methodologies to include but not be limited to lecture, hands-on assignments, discussion forums, and projects that can be either individually or group assigned.

Reading Assignments

Weekly reading assignments will be given from the required text or online materials provided by web links via the instructor.

Writing Assignments

Written assignments will include discussion forum posts and short essay responses.

Out-of-class Assignments

Assignments will consist of quizzes, labs, and discussion questions.

Demonstration of Critical Thinking

Troubleshooting of hacking tools.

Required Writing, Problem Solving, Skills Demonstration

Install and configure various Network Security software and hardware. Demonstrate how to use this software and hardware in a virtual environment.

Eligible Disciplines

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

Textbooks Resources

1. Required Oriyano, Sean-Philip; Solomon, Michael. Hacker Techniques, Tools, and Incident Handling, 3rd ed. Burlington, MA: Jones Bartlett Learning, 2020 Rationale: -

Other Resources

1. Coastline Library