CYBR C271: BECOME A SECURITY CONSULTANT

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
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Formerly: CST C271. This course introduces the concepts of professional security consulting for students with prior security training and work experience. Topics covered include types of security consulting, qualifications, setting up practice and finding clients, security tools and audits, and ethics for security consultants. The fundamentals of security consulting for private and government organizations are surveyed. Hands-on exercises using industry-recognized tools for security audit and assessment help students develop skills to prepare for a career as a Security Consultant. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Define the terminology associated with Security Consulting and explain the steps that need to be taken to become a Security Consultant.
2. Demonstrate proficiency using various tools used by a professional Security Consultant.
3. Given a scenario, design a work plan describing what steps should be taken to perform a security assessment, identify the tools to be used, and explain why those steps and tools were selected.

Course Objectives

- 1. Identify the skills and characteristics of a security consultant.
- 2. Demonstrate use of security consulting tools to identify security vulnerabilities and provide companies with solutions to common issues.
- 3. Outline the steps required to conduct a security audit including contracts and requirements for permission.
- 4. Explain the types of training and certification needed for security consulting roles in private business and government organizations.
- 5. Analyze ethical concerns, legal implications, and confidentiality requirements related to security consulting.

Lecture Content

What is a Security Consultant. Characteristics of a Consultant Types of Security Consulting Qualifications for a Security Consultant Training and Certifications Personal characteristics Becoming a Security Consultant Setting up a practice Finding clients Tools used by a Security Consultant Hardware tools Software tools Performing a Security Audit Permissions needed Designing a plan Forensics Consulting Containing the damage Tracking the damage Mitigating the damage Correcting the vulnerabilities Security Consulting for a Private Organization Types of organizations Working with a companies security organization Security Consulting for a Government Organization Types of organizations Security clearances Training to Become a Security Consultant On-the-job Job shadowing Professional organizations The Ethics of Security Consulting Consulting and the law Confidentiality

Lab Content

Capture and analyze network traffic Apply and implement a secure network configuration Perform log analysis Connect to a remote system Analyze wireless network traffic Setup a virtual private network (VPN)

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, remote virtual machine 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 articles outlining the steps to become a Security Consultant. Read articles and review professional organization sites that provide detailed requirements for training and industry-recognized certifications for cybersecurity professionals. Read the course assigned textbook and articles that debate and discuss ethical situations encountered in cybersecurity work roles. Read the course assigned textbook and articles that explain situations encountered regarding privacy and confidentiality in cybersecurity professional roles.

Writing Assignments

Create a plan for performing a security audit, including the tools to be used.

Out-of-class Assignments

Conduct a security assessment using remote lab environment. Discuss standard security policies and common procedures and practices.

Demonstration of Critical Thinking

Assess organizational security using appropriate hardware and software tools.

Required Writing, Problem Solving, Skills Demonstration

Students will demonstrate the ability to use various security tools to protect networked systems. Students will discuss security consulting

ethics, legal implications, and security assessment methodologies to meet industry needs.

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.

Other Resources

1. Coastline Library 2. IT white papers are available at no charge to all IT students through the Microsoft IT Academy website.