California State University, Long Beach
College of Business

Standard Course Outline
IS 460 Defensive Cybersecurity in Business

I. General Information

- Course number: IS 460
- Title: Defensive Cybersecurity Operations
- Units: 3
- Prerequisites: IS 360 or IS 456
- Course Coordinator: Dr. Spiro Samonas
- SCO Prepared by: Dr. Spiro Samonas
- Date prepared/revised: 3/23/2018

II. Catalog Description

Advanced business and management applications of defensive cybersecurity operations. Incident response and computer forensics. Computer network defense. Cryptography. Penetration testing. Malware attacks. Configuration management. Individual project. Letter grade only (A-F).

III. Curriculum Justification(s)

Across different countries and industries, the average data breach costs millions of US dollars every year. Businesses need to protect information systems and the information contained therein from damage, unauthorized use or modification, or exploitation. To achieve this, appropriate incident response mechanisms, as well as technical safeguards, such as firewalls and intrusion prevention systems, help businesses detect, prevent, and/or mitigate costly security breaches. Security information and event management teams develop and implement a coordinated and structured response to security incidents that focus on the swift and accurate investigation, resolution and remediation of security breaches in business.

This course is a necessary addition to the Information Systems curriculum that builds upon the information assurance aspects of cybersecurity that are covered in IS 360 - Introduction to Cybersecurity in Business. Students will gain hands-on knowledge of key defensive operations of cybersecurity in business, such as computer network defense, penetration testing and computer forensic evidence collection and analysis. The course draws relevant knowledge from Information Systems, Computer Science, Psychology, and Criminology.

IV. CBA Undergraduate Program Learning Goals:

General Learning Goals

- **Critical Thinking**: Students will be able to demonstrate conceptual learning, critical thinking, and problem-solving skills. Students will be able to:
    - Perform a digital crime scene investigation by collecting and analyzing computer forensic evidence in a business context. Students will then be asked to present and

defend their findings against concerns, such as chain of custody violations and evidence tampering.

- **Ethics**: Students will be able to demonstrate awareness and knowledge of social responsibility, ethical leadership, and citizenship issues in the local, regional and world communities. Students will be able to:
    - Demonstrate understanding of the legal and ethical aspects of penetration testing in a business context.
- **Interpersonal, Leadership & Team Skills**: Students will be able to demonstrate interpersonal and leadership skills for working in a dynamic and diverse world, both independently and in a team environment. Students will be able to:
    - Manage an individual project and deliver a written report and a formal presentation in front of their class peers.

Management-Specific Learning Goals

- **Business Functions**: Students will be able to demonstrate understanding of a broad spectrum of business functions, practices and related theories and be able to integrate this functional knowledge in order to address business problems. Students will be able to:
    - Recognize the added value that defensive cybersecurity operations such as vulnerability scanning, and penetration testing offer to business. This will be achieved by understanding the relationship between a) asset identification and valuation, b) known attacks, threats and vulnerabilities, and how the latter translate into a tangible (quantifiable) or intangible (e.g. business reputation) risk.
- **Quantitative & Technical Skills**: Students will possess quantitative and technological skills enabling them to analyze, interpret, and communicate business data effectively and to improve business operations. Among other technical skills, students will learn to:
    - Perform penetration testing using Kali Linux or a similar environment.
    - Collect and analyze different types of computer forensic evidence.
    - Perform network protocol analysis.

V. Course Objectives, Student Learning Outcomes, Evaluation Instruments, and Instructional Strategies for Skill Development

OBJECTIVE 1: Perform basic penetration testing tasks using Kali Linux or a similar environment.

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to use an assortment of applications in Kali Linux, such as Nmap, Dmitry, Wireshark and Metasploit to complete different aspects of a penetration test.
- ***EVALUATION INSTRUMENTS***: Specific assignments will vary by instructor, but typical assignments include lab assignments and in-class exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A lab assignment rubric evaluating the ability of students to use applications in Kali Linux will be provided. Performance expectations and standards will be discussed in class before and after any lab assignments.

OBJECTIVE 2: Conduct a computer forensic investigation using the SANS Investigative Forensics Toolkit or a similar environment.

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to collect and analyze computer forensic evidence using SIFT, while ensuring that the evidence will be admissible in a court of law.
- ***EVALUATION INSTRUMENTS***: Specific assignments will vary by instructor, but typical assignments include lab assignments based on mock digital crime scenes, and in-class exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A written assignment rubric evaluating the ability of students to collect and analyze computer forensic evidence will be used. Performance expectations and standards will be discussed in class before and after any lab assignments.

OBJECTIVE 3: Learn to work with task automation and configuration management scripts using Windows PowerShell or a similar application.

- ***MEASURABLE OUTCOME***: After taking this course, students will be able to use Windows PowerShell for cybersecurity related tasks.
- ***EVALUATION INSTRUMENTS***: Specific assignments will vary by instructor, but typical assignments include lab assignments and in-class exams.
- ***INSTRUCTIONAL STRATEGIES FOR SKILL DEVELOPMENT***: A written assignment rubric evaluating the ability of students to use Windows PowersShell will be used. Performance expectations and standards will be discussed in class before and after any lab assignments.

VI. Outline of Subject Matter

The topic outline for the course is the following. Subject matter and sequence of topics may vary by instructor.

1. Overview of Information Assurance and Cybersecurity
2. Networks and Telecommunications in Business
3. Overview of the Cyber Kill Chain Model
4. Penetration Testing (Reconnaissance, Vulnerability Mapping, Network Protocol Analysis, Wireless Security Testing)
5. Computer Network Defense
6. Cybersecurity Laws and Law Enforcement
7. Computer Forensics (Bitstream Imaging and Image Analysis, Volatile Memory Analysis, Network Forensics)
8. Task Automation and Configuration Management for Cybersecurity
9. Cryptography
10. Optional additional topics include: Social Engineering

VII. Methods of Instruction

INSTRUCTION MODE

As per the University policies Academic Technology and the Mode of Instruction (PS 03-11) and Course Syllabi and Standard Course Outlines (PS 11-07) that pertain to modes of instruction, this course is authorized to use the traditional mode of instruction that involves face-to-face class sessions.

CLASSROOM ACTIVITIES

The course has four main components: (1) lecture and readings, (2) case analyses, (3) homework and lab assignments, and (4) an individual project. Students are required to actively participate in in-class discussions, work individually and in groups, and develop their technical skills. Student will be evaluated using case reports, lab assignments, oral presentations, an individual project, and three exams. For both written and oral tasks, feedback will be provided to students regularly to support their continuous improvement.

EXTENT AND NATURE OF TECHNOLOGY USE.

Instructors will assign homework and in-class assignments involving the use of hardware and software, as well as projects on information systems security.

VIII. Information about Textbooks/Readings

The following is a short list of textbooks that are suggested for this course. Instructors may assign one or more of these and/or include other relevant texts/readings. Instructors may be asked to justify the use of old textbooks, if updated texts are available:

- Luttgens, J., Pepe, M., & Mandia, K. (2014) "*Incident Response & Computer Forensics*", McGraw Hill Professional.
- Ciampa, M. (2015) "CompTIA Security+ Guide to Network Security Fundamentals, 5th Edition", Cengage Learning ISBN-13: 9781305093911.
- Whitman, M. E., & Mattord, H. J. (2014) "*Hands-on Information Security Lab Manual, 4th Edition*". Cengage Learning.

IX. Instructional Policies Requirements

Every course should comply with the relevant Academic Senate Policy Statements. Instructional policies should be consistent with the course description outlined in Sections II and III, and should serve the course objectives listed in section IV of this SCO. Specific attendance and late assignment policies are up to the discretion of each instructor, as long as these policies follow the Academic Senate Policy Statements. The same applies if some or all sections of the course are to be taught, in part or entirely, by distance learning in the future.

Students are expected to abide with the following policies that are outlined in the CSULB Catalog:

- The Standards for Student Conduct

- Academic Integrity Regarding Cheating and Plagiarism
- The withdrawal policy

X. Course Assessment and Grading (Optional but highly recommended for core courses)

DESCRIPTION OF ASSESSMENT

The suggested workload and grading for this course is as follows:

Assignment Description	% of Course Grade
Project	15%
In-class Assignments and Homework	30%
Mid-term Exam 1	15%
Mid-term Exam 2	15%
Final Exam	15%
Total:	100%

GRADING POLICIES AND PROCEDURES

Grading policies, procedures, and the percentage of the course grade associated with each assessment must be explicit on each instructor's syllabus and must be consistent with University policy on Final Course Grades, Grading Procedures, and Final Assessments (PS 12-03). Instructors must develop scoring guidelines for assessments, which must be made available to students. The final course grade will be based on a descriptive scale such as the following:

Percentage	Letter Grade	Description of Grade
90-100%	A	Mastery of the relevant course standards.
80-89%	B	Above average proficiency of the relevant course standards.
70-79%	C	Satisfactory proficiency of the relevant course standards.
60-69%	D	Partial proficiency of the relevant course standards.
Below 60%	F	Little or no proficiency of the relevant course standards.

XI. Disabilities

The Bob Murphy Access Center (BMAC) provides certification for students with disabilities and helps arrange relevant accommodations. Any student requesting academic accommodations based on a disability is strongly encouraged to register with Disabled Student Services (BMAC) each semester. A letter of verification for approved accommodations can be obtained from BMAC. Please be sure to provide your instructor with BMAC verification of accommodations as early in the semester as possible. The phone number for BMAC is (562) 985 5401. The email address is: bmac@csulb.edu.

XII. Assistive Technology

In compliance with Accessibility and Faculty Responsibility for the Selection of Instructional Materials (PS 08-11), instructors are responsible for ensuring that their syllabi and instructional materials are accessible to all students.

XIII. Consistency of SCO Standards across Sections

All future syllabi will conform to the SCO. The course coordinator should review the SCO and offer advice and/or materials to faculty member new to teaching the course. The course coordinator may offer or require regular review of instructors' course materials as well as anonymous samples of student work.

XIV. Additional Resources for Development of Syllabi

- Academic Senate Policy 11-07: Course Syllabi and Standard Course Outlines
- College of Business Accessible Syllabus Template
- Faculty Center Course and Syllabus Design