College of San Mateo
Official Course Outline

1. **COURSE ID:** CIS 482 **TITLE:** Ethical Hacking
Units: 3.0 units **Hours/Semester:** 48.0-54.0 Lecture hours; and 96.0-108.0 Homework hours
Method of Grading: Grade Option (Letter Grade or Pass/No Pass)
Prerequisite: CIS 151
Recommended Preparation:
Eligibility for ENGL 838 or ENGL 848 or ESL 400.
CIS 110

2. **COURSE DESIGNATION:**
Degree Credit
Transfer credit: CSU

3. **COURSE DESCRIPTIONS:**
Catalog Description:
Students will scan, test, hack and secure systems. Implement perimeter defenses, scan and attack virtual networks. Other topics include intrusion detection, social engineering, footprinting, DDoS attacks, buffer overflows, SQL injection, privilege escalation, trojans, backdoors and wireless hacking. Legal restrictions and ethical guidelines emphasized. This course also helps prepare students to pass the Certified Ethical Hacker (C|EH) exam.

4. **STUDENT LEARNING OUTCOME(S) (SLO'S):**
Upon successful completion of this course, a student will meet the following outcomes:
1. Demonstrate the ability to attack and defend a network.
2. Investigate how to attack a computer system
3. Perform penetration testing
4. Explore hacking through the network: Sniffers and evasion

5. **SPECIFIC INSTRUCTIONAL OBJECTIVES:**
Upon successful completion of this course, a student will be able to:
1. Gather information for the ethical hacking, vulnerability research and Footprinting
2. Explore scanning and enumeration on targets
3. Explore hacking through Sniffers, evasion Sniffing and network roadblocks
4. Investigate trojans, backdoors, viruses, worm attacks, denial of service attacks and session hijacking
5. Perform penetration testing

6. **COURSE CONTENT:**
Lecture Content:
A. Explore ethical hacking basics
1. Introduction to Ethical Hacking
2. Legal hacking: Laws and guidelines
B. Explore cryptography
1. Cryptography and encryption overview
2. PKI, the digital certificate, and digital signatures
3. Encrypted communication and cryptography attacks
C. Investigate reconnaissance: Information gathering for the ethical hacker
1. Vulnerability research
2. Footprinting
D. Explore scanning and enumeration
1. Scanning for targets
2. Enumeration
E. Explore hacking through the network: Sniffers and evasion
1. Sniffing
2. Network roadblocks
A. Intrusion detection
B. Firewall and honeypots
F. Investigate how to attack a computer system

1. Windows system hacking
2. Linux hacking

G. Explore low tech hacking techniques

1. Social engineering
2. Physical security

H. Investigate web-based hacking

1. Attacking web servers
2. Attacking web applications

I. Explore wireless network hacking

1. Wireless Concepts
    A. Network architecture and standards
    B. Finding and identifying wireless networks
2. Wireless hacking
    A. Wireless attacks
    B. Bluetooth attacks

J. Investigate trojans and other attacks

1. Trojans, backdoors, viruses, and worm attacks
2. Denial of service attacks
3. Session hijacking

K. Perform penetration testing

1. Methodology and Steps
    A. The security assessments
    B. Security assessment deliverables
2. Information Gathering and Analysis

7. **REPRESENTATIVE METHODS OF INSTRUCTION:**
   Typical methods of instruction may include:
   A. Lecture
   B. Lab
   C. Activity
   D. Discussion
   E. Observation and Demonstration
   F. Other (Specify): In class problem-solving. Class (group) problem-solving. Q/A sessions with students. Quiz and examination review performed in class.

8. **REPRESENTATIVE ASSIGNMENTS**
   Representative assignments in this course may include, but are not limited to the following:
   Writing Assignments:
   Students will be assigned weekly homework problems from the required textbook. Approximately four extensive analysis projects will be assigned which require problem solving and critical thinking. Students will write a report for each project. Students also will create and deliver presentations.
   Reading Assignments:
   Students will read all chapters of the required textbook, readings parallel current assignments, and lecture content. Extensive web searching is critical.
   Other Outside Assignments:
   Weekly homework problems, internet research, and working on presentations.

9. **REPRESENTATIVE METHODS OF EVALUATION**
   Representative methods of evaluation may include:
   A. Class Participation
   B. Class Performance
   C. Class Work
   D. Exams/Tests
   E. Group Projects
   F. Homework
   G. Projects
   H. Quizzes
   I. Research Projects

10. **REPRESENTATIVE TEXT(S):**
    Possible textbooks include:

A. Walker, Matt. *CEH Certified Ethical Hacker Boxed Set*, 1 ed. McGraw-Hill USA, 2013
B. Kim, Peter. *The Hacker Playbook (Book 3)*, ed. Independently published, 2018

Origination Date: March 2017
Curriculum Committee Approval Date: September 2018
Effective Term: Fall 2019
Course Originator: Kamran Eftekhari