## I. CATALOG INFORMATION

A. Discipline: COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

B. Subject Code and Number: CNSE M84

C. Course Title: Certified Ethical Hacker

D. Credit Course units:

Units: 3

Lecture Hours per week: 2

Lab Hours per week : 3

Variable Units : No

E. Student Learning Hours:

Lecture Hours:

Classroom hours: 35 - 35

Laboratory/Activity Hours:

Laboratory/Activity Hours 52.5 - 52.5

**Total Combined Hours** in a 17.5 week term: 87.5 - 87.5

F. Non-Credit Course hours per week __________

G. May be taken a total of: ☒ 1 □ 2 □ 3 □ 4 time(s) for credit

H. Is the course co-designated (same as) another course: No ☒ Yes □
If YES, designate course Subject Code & Number: __________

I. Course Description:

Provides training using the latest tools, techniques, and exploits used in network penetration. Focuses on students' performance in labs related to digital reconnaissance, hacking strategies, bypassing intruder detection systems, firewall management, network sniffing, and testing of security settings on Windows and Linux systems.

J. Entrance Skills

*Prerequisite: No ☒ Yes □ Course(s)
__________

*Corequisite: No ☒ Yes □ Course(s)
__________

Limitation on Enrollment: No ☒ Yes □
__________

Recommended Preparation: No □ Yes ☒ Course(s)
CNSE M13 and CNSE M55

Other: No ☒ Yes □
__________

K. Other Catalog Information:

Course prepares students to pass the Certified Ethical Hacker exam given by the EC-Council.

## II. COURSE OBJECTIVES

Upon successful completion of the course, a student will be able to:

| | | **Methods of evaluation will be consistent with, but not limited by, the following types or examples.** |
|---|---|---|
| 1 | describe what computer and network forensics is about, what is an Ethical Hacker, and practice Best Practices in safe use of the Internet, and public and private systems. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 2 | describe hacking techniques including reconnaissance methods, information gathering, and social engineering. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 3 | compare operating systems, wired and wireless networks, and web application vulnerabilities. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 4 | discuss various methods of attack and methods of mitigation or protection including denial of service, password cracking, trojans and backdoors, and network sniffing. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 5 | discuss modern electronic tools used to gather, save, and process evidence. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 6 | describe various attack detection and attack hiding techniques. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| | | Quizzes |

| | | |
|---|---|---|
| 7 | describe ways hostile codes are used to gain unauthorized access to computer network systems. | Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 8 | defend a computer and a Local Area Network against using Intruder Detection Systems, Firewalls, Honeypots, and other methods of evasion. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 9 | discuss forensic issues relevant to Linux, Apple, and Microsoft environments. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |
| 10 | describe some of the prominent computer crime laws such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act. | Quizzes<br>Midterms and final exam<br>Classroom project work demonstrating competency in this area |

## III. COURSE CONTENT

| Estimated % | Topic | Learning Outcomes |
|---|---|---|
| **Lecture** (must total 100%) | | |
| 5.00% | Conducting ethical hacking<br>- Ethics<br>- Legality | 1 |
| 10.00% | Footprinting, scanning, and enumeration | 2, 6 |
| 5.00% | System hacking | 2, 4, 5, 6 |
| 5.00% | Trojans and backdoors and buffer overflows | 4, 7 |
| 5.00% | Sniffers | 3, 4, 5 |
| 5.00% | Denial Of Service (DOS) attacks | 4, 5, 6, 7 |
| 3.00% | Session hijacking | 4, 5, 6, 7 |
| 5.00% | Transmission Control Protocol Internet Protocol (TCP/IP) and Web application vulnerabilities | 5, 6, 7, 8 |
| 5.00% | Password cracking | 3, 4, 5, 6, 7 |
| 5.00% | Structured query language (SQL) injection | 4, 5, 6, 7, 8, 9 |
| 5.00% | Wireless hacking | 3, 4, 5, 6, 8 |
| 5.00% | Virus and worms | 5, 6, 7, 8 |

| | | |
|---|---|---|
| 3.00% | Physical security | 3, 4, 5, 6, 7, 8, 9 |
| 5.00% | Honeypots, Intruder Detection Systems, Firewalls, and Security Devices | 6, 7, 8, 9 |
| 5.00% | Cryptography | 6, 7, 9, 10 |
| 5.00% | Penetration testing methodologies | 3, 4, 5, 6, 7, 8 |
| 5.00% | Windows, Linux, and embedded operating system hacking | 8, 9 |
| 5.00% | Social engineering | 2, 4, 5, 6, 9, 10 |
| 5.00% | Hacking web servers and web applications | 4, 5, 6, 7, 8, 9, 10 |
| 4.00% | Programming for Security Professionals | 2, 3, 4, 6, 8 |
| **Lab** (must total 100%) | | |
| 5.00% | Common Vulnerabilities and Exposures website (CVE) and National Security Agency website | 1, 2, 3, 4 |
| 10.00% | Network Mapping (NMAP) for network penetration scanning. Note: All labs to be performed in a sandbox isolated environment. Academic license for 3rd party website that provides pre-configured classroom labs at external sandbox site | 2, 3, 8, 9 |
| 15.00% | Scanning, enumeration and reconnaissance | 2, 3, 4, 5, 6, 7, 8, 9 |
| 10.00% | Network sniffing for packet captures | 2, 3, 4, 5, 6, 7, 8, 9 |
| 10.00% | Isolated and focused hacking attack techniques against specific systems | 3, 4, 5, 7, 8 |
| 10.00% | Isolated hacking on computer hosts, servers and web applications | 4, 5, 6, 7, 8 |
| 10.00% | Isolated wireless hacking techniques | 3, 4, 5 |
| 5.00% | Isolated trojan and virus attacks | 4, 5, 6 |
| 10.00% | Hashing and encryption methods to verify information confidentiality and integrity | 1, 2, 3, 5, 6, 10 |
| 15.00% | Penetration testing against a variety of isolated systems | 2, 3, 4, 5, 6, 7, 8, 9 |

## IV. TYPICAL ASSIGNMENTS

### A. Writing assignments

| | |
|---|---|
| Writing assignments are required. Possible assignments may include, but are not limited to: | |
| 1 | write about problems and solutions in an engineering journal while performing penetration testing labs. |
| 2 | write explanations which demonstrate knowledge in security mitigation techniques. |

### B. Appropriate outside assignments

| | |
|---|---|
| Appropriate outside assignments are required. Possible assignments may include, but are not limited to: | |

| | |
|---|---|
| 1 | research Common Vulnerabilities and Exposures Website (CVE) which post vulnerabilities detected on the Internet and is subscribed to by companies for ongoing threat protection. |
| 2 | review National Security Agency for published recommendations including executive summaries, and extensive configuration guides on how to properly secure a variety of network connected devices, including various operating systems and web applications. |

C. Critical thinking assignments

| | |
|---|---|
| Critical thinking assignments are required. Possible assignments may include, but are not limited to: | |
| 1 | discuss lab solutions with lab partners that demonstrate problem solving skills. |
| 2 | solve lab scenarios to meet business requirements, such as threat mitigation techniques that detect, log, and protect a network connected system. |

## V. METHODS OF INSTRUCTION

Methods of instruction may include, but are not limited to:

☒ Distance Education – When any portion of class contact hours is replaced by distance education delivery mode (Complete DE Addendum, Section XV)

☒ Lecture/Discussion

☒ Laboratory/Activity

☒ Other (Specify)
Use of virtualized, isolated, and sandboxed environments to train students on how to test security methods in a lab test environment.

☐ Optional Field Trips

☐ Required Field Trips

## VI. METHODS OF EVALUATION

**Methods of evaluation may include, but are not limited to:**

☐ Essay Exam

☒ Problem Solving Exam

☒ Objective Exams

☒ Classroom Discussion

☒ Reports/Papers/ Journals

☒ Projects

☒ Skill Demonstration

☒ Participation

☒ Other (specify)

Evaluation will include traditional assessment of theory but will also include assessment through various lab scenarios.

## VII. REPRESENTATIVE TEXTS AND OTHER COURSE MATERIALS

Simpson, Michael T., and Nicholas Antill. Hands-On Ethical Hacking and Network Defense. 3rd ed. Cengage, 2017.

International Council of E-Commerce Consultants (EC-Council). Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures. 2nd ed.

Cengage, 2017.

## VIII. STUDENT MATERIALS FEES

☒ No □ Yes

## IX. PARALLEL COURSES

| *College* | *Course Number* | *Course Title* | *Units* |
|---|---|---|---|
| Coastline Community College | C S T 232 | Ethical Hacking | 3-9 |
| Fresno City College | CIT 58F | Ethical Hacking | 3 |
| Mt. San Antonio College | CISS 21 | Network Vulnerabilities and Countermeasures | 3 |

## X. MINIMUM QUALIFICATIONS

**Courses in Disciplines in which Masters Degrees are not expected:**
Associate Degree and 6 years networking experience and CCNA, MCSA, or Certified Ethical Hacker certification, or 2 years experience in Computer Security.

## XI. ARTICULATION INFORMATION

A. Title V Course Classification:

1. This course is designed to be taken either:

   □ Pass/No Pass only (no letter grade possible); or
   ☒ Letter grade (P/NP possible at student option)

2. Degree status:
   Either ☒ Associate Degree Applicable; or □ Non-associate Degree Applicable

B. Moorpark College General Education:

1. Do you recommend this course for inclusion on the Associate Degree General Education list?
   Yes: □ No: ☒ If YES, what section(s)?

   □ A1 - Natural Sciences - Biological Science
   □ A2 - Natural Sciences - Physical Science
   □ B1 - Social and Behavioral Sciences - American History/Institutions
   □ B2 - Social and Behavioral Sciences - Other Social Behavioral Science
   □ C1 - Humanities - Fine or Performing Arts
   □ C2 - Humanities - Other Humanities
   □ D1 - Language and Rationality - English Composition
   □ D2 - Language and Rationality - Communication and Analytical Thinking
   □ E1 - Health/Physical Education
   □ E2 - PE or Dance
   □ F - Ethnic/Gender Studies

C. California State University(CSU) Articulation:

1. Do you recommend this course for transfer credit to CSU? Yes: □ No:

☒

2. If YES do you recommend this course for inclusion on the CSU General Education list?
   Yes: □ No: ☒ If YES, which area(s)?

   A1 □ A2 □ A3 □ B1 □ B2 □ B3 □ B4 □

   C1 □ C2 □ D1 □ D2 □ D3 □ D4 □ D5 □
   D6 □ D7 □ D8 □ D9 □ D10 □ E □

D. University of California (UC) Articulation:

1. Do you recommend this course for transfer to the UC? Yes: □ No: ☒

2. If YES do you recommend this course for the Intersegmental General Education Transfer Curriculum (IGETC)? Yes: □ No: ☒

   IGETC Area 1: English Communication

   □ English Composition
   □ Critical Thinking-English Composition
   □ Oral Communication

   IGETC Area 2: Mathematical Concepts and Quantitative Reasoning

   □ Mathematical Concepts

   IGETC Area 3: Arts and Humanities

   □ Arts
   □ Humanities

   IGETC Area 4: Social and Behavioral Sciences

   □ Anthropology and Archaeology
   □ Economics
   □ Ethnic Studies
   □ Gender Studies
   □ Geography
   □ History
   □ Interdisciplinary, Social & Behavioral Sciences
   □ Political Science, Government & Legal Institutions
   □ Psychology
   □ Sociology & Criminology

   IGETC Area 5: Physical and Biological Sciences (mark all that apply)

   □ Physical Science Lab or Physical Science Lab only (none-sequence)
   □ Physical Science Lecture only (non-sequence)

□ Biological Science

□ Physical Science Courses

□ Physical Science Lab or Biological Science Lab Only (non-sequence)

□ Biological Science Courses

□ Biological Science Lab course

□ First Science course in a Special sequence

□ Second Science course in a Special Sequence

□ Laboratory Activity

□ Physical Sciences

IGETC Area 6: Language other than English

□ Languages other than English (UC Requirement Only)

□ U.S. History, Constitution, and American Ideals (CSU Requirement ONLY)

□ U.S. History, Constitution, and American Ideals (CSU Requirement ONLY)

## XII. REVIEW OF LIBRARY RESOURCES

A. What planned assignment(s) will require library resources and use?

The following assignments require library resources:
Access to Library research materials and journal articles, online and in print, which discuss such topics as how to properly secure a variety of network connected devices.

B. Are the currently held library resources sufficient to support the course assignment?

YES: ☒ NO: □

If NO, please list additional library resources needed to support this course.

## XIII. PREREQUISITE AND/OR COREQUISITE JUSTIFICATION

CNSE M84: Not Applicable

## XIV. WORKPLACE PREPARATION

Required for career technical courses only. A career technical course/program is one with the primary goal to prepare students for employment immediately upon course/program completion, and/or upgrading employment skills.

Detail how the course meets the Secretary of Labors Commission on the Achievement of Necessary Skills (SCANS) areas. (For a description of the competencies and skills with a listing of what students should be able to do, go to: http://www.ncrel.org/sdrs/areas/issues/methods/assment/as7scans.htm)

The course will address the SCANS competency areas:

1. Resources: the students will identify, organize, plan, and allocate resources through course work and application of theory to practice.

2. Interpersonal: the students will work together as a team to build and evaluate

projects, and solve technical problem scenarios.

3. Information: the students will acquire and use information through a variety of assignments, network technology tools, and computer software used in securing network systems.

4. Systems: the students will employ a variety of computer security tools to complete projects or assess security problems.

5. Technology: the students will use modern technology to acquire the skills needed to secure a system.

The course also addresses the SCANS skills and personal qualities:

1. Basic Skills: the students will read, perform computer and network analysis operations, listen, and speak in weekly assignments and participate in classroom discussions.

2. Thinking Skills: the students will think creatively and make decisions in order to solve computer network security problems and demonstrate reasonable problem solving skills.

3. Personal Qualities: the students will be required to display responsibility, self-management, integrity, and honesty throughout course work and classroom exercises. Students will adhere to the rules of engagement when performing ethical hacking or penetration testing activities by only assessing test networks in a sandbox environment and not using tools against production networks.

## XV. DISTANCE LEARNING COURSE OUTLINE ADDENDUM

1. Mode of Delivery

   ☒ Online (course will be delivered 100% online)

   ☒ Online with onsite examinations (100% of the instruction will occur online, but examinations and an orientation will be scheduled onsite)

   ☒ Online/Hybrid (a percentage of instruction will be held online and the remaining percentage of instruction will be held onsite)

   ☒ Lab activities will be conducted onsite

   □ Televideo (Examinations and an orientation will be held onsite)

   □ Teleconference

   □ Other

2. Need/Justification

   Improve general student access.

3. Describe how instructors teaching this course will ensure regular, effective contact with and among students.

   Online instructors will provide lesson modules that require activities such as reading course material, performing online labs, and participating in discussion forums or chat room topics. Instructors may also meet with students for study sessions and online office hours using an online communication tool. Instructors will provide students with feedback on the content and quality of assignments and discussion posts. Additionally, instructors may engage students using the following communication activities available in the online classroom: contact students via e-mail within the course shell, by campus e-mail, and/or MyVCCCD; use the "announcement" tool to remind students of important assignments and due dates; provide students with an online schedule of class events using the "calendar" tool in the online course shell and including due dates in Canvas modules link.

4. Describe how instructors teaching this course will involve students in active learning.

   Instructors may involve students in active learning with the following activities: students may view video lessons and/or text-based lessons corresponding to course content and learning objectives; students may complete homework through the online course, and/or using an interactive online homework system provided by a curriculum vendor; students may engage in internet searches and library online database resources on topics corresponding to course content and learning objectives; students may test their knowledge with interactive online quizzes; students may interact with the instructor and classmates using an online discussion forum to ask questions; students may submit questions to the instructor by email or ask in person in a virtual classroom; instructor may create student groups or group activities using the online course.

5. Explain how instructors teaching this course will provide multiple methods of content representation.

   The following represent the methods by which content may be provided for learning: instructional videos; textbook and online professional curriculum; links to online resources that may include videos, quizzes, text explanations, homework assignments; labs supporting chapter content.

6. Describe how instructors teaching this course will evaluate student performance.

   Lab assignments, various quizzes and exams.

   Students may take objective and essay exams in an online teaching environment. Students may be required to do the following assignments: perform online lab final measuring mastery of course content; develop a penetration testing strategy for a specific technical environment, complete regular online quizzes; complete written assignments related to key course concepts; participate in online discussion forums.

## XVI. GENERAL EDUCATION COURSE OUTLINE ADDENDUM

CNSE M84: Not Applicable

## XVII. STUDENT MATERIALS FEE ADDENDUM

CNSE M84: Not Applicable

## XVIII. REPEATABILITY JUSTIFICATION TITLE 5, SECTION 55041

CNSE M84: Not Applicable

## XIX. CURRICULUM APPROVAL

Course Information:

Discipline:

COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

Discipline Code and Number: CNSE M84

Course Revision Category: Technical Course Revision

Course Proposed By:

Originating Faculty ______

Faculty Peer: ______

Curriculum Rep: ______

Department Chair: ______

Division Dean: ______

Approved By:

Curriculum Chair: ______

Executive Vice President: ______

Articulation Officer: ______

Librarian: ______

Implementation Term and Year: Fall 2017

Approval Dates:

Approved by Moorpark College Curriculum Committee: 03/07/2017

Approved by Board of Trustees (if applicable): 04/11/2017

Approved by State (if applicable): 04/24/2017