## I. CATALOG INFORMATION

A. Discipline: COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

B. Subject Code and Number: CNSE M82

C. Course Title: Introduction to Network Security

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 a comprehensive overview of network security. Covers general security concepts, communication security, infrastructure security, cryptography, and operational/organizational security needs.

J. Entrance Skills

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

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

Limitation on Enrollment: No ☒ Yes □
_________

Recommended Preparation: No □ Yes ☒ Course(s)
Proficiency using computers for Internet research.

Other: No ☒ Yes □
_________

K. Other Catalog Information:

Prepares students for Computing Technology Industry Association (CompTIA) Security+ certification exam. align with C-ID: ITIS 160

## 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 principles of information systems security including threat trends and their ramifications including appropriate strategies to assure confidentiality, integrity, and availability of information. | Quizzes<br>Mmidterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 2 | determine both technical and administrative mitigation approaches including what mutual authentication is and why it is necessary. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 3 | define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related including risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 4 | discuss the different vulnerabilities associated with telecommuting. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, |

| | | |
|---|---|---|
| | | presentations, discussions, or problem solving assignments |
| 5 | perform risk analysis and risk management and create and maintain a comprehensive security model. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 6 | explain the vulnerabilities of JavaScript, buffer overflow, ActiveX, cookies, Common Gateway Interface (CGI), applets, Simple Mail Transfer Protocol (SMTP) relay, and how they are commonly exploited. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 7 | explain the benefits offered by centralized enterprise directory services such as Lightweight Directory Access Protocol (LDAP) over traditional authentication systems. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 8 | describe the Wireless Transport Layer Security (WTLS) Protocol and how it works. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| | | Quizzes |

| | | |
|---|---|---|
| 9 | explain the purpose of a network firewall and the different kinds of firewall technology available on the market. | Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 10 | evaluate the need for the careful design of a secure organizational information infrastructure. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 11 | explain the network perimeter’s importance to an organization’s security policies. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 12 | explain what intrusion detection systems are and identify some of the major characteristics of intrusion detection products. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 13 | identify network services that are commonly exploited by attackers. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a |

| | | |
|---|---|---|
| | | combination of examinations, presentations, discussions, or problem solving assignments |
| 14 | discuss the characteristics of Public Key Infrastructure (PKI) certificates and the policies and procedures surrounding them and define basic cryptography, its implementation considerations, and key management. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 15 | discuss the impact of location on a facility's security. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |
| 16 | explain the importance of defining and documenting security policies and procedures. | Quizzes<br>Midterms<br>Final exam<br>Classroom project work demonstrating competency in this area including hands-on projects and a combination of examinations, presentations, discussions, or problem solving assignments |

## III. COURSE CONTENT

| Estimated % | Topic | Learning Outcomes |
|---|---|---|
| **Lecture** (must total 100%) | | |
| 6.00% | Disaster Recovery and Business Continuity | 1, 2, 3, 4, 11, 16 |
| 8.00% | Security Overview | 1, 2, 3, 4, 5, 13, 14, 16 |
| 8.00% | Authentication and Account Management | 2, 4, 7, 16 |

| | | |
|---|---|---|
| 8.00% | Attacks, Malicious Code, Malware, Social Engineering | 1, 3, 5, 6, 9, 11, 12, 13, 16 |
| 8.00% | Security Administration | 1, 4, 5, 13, 15, 16 |
| 7.00% | Application and Network Security | 2, 3, 5, 6, 7, 9, 11, 13 |
| 7.00% | Vulnerability Assessment and Mitigation | 9, 10, 11, 13, 14, 15 |
| 7.00% | Network Security Topologies | 3, 4, 9, 10, 11, 12, 13, 14, 15 |
| 10.00% | Host, Application, Data Security and Intruder Detection Systems | 4, 6, 7, 8, 10, 11, 12, 13, 14, 16 |
| 7.00% | Security Baselines | 1, 4, 9, 10, 11, 12, 13, 16 |
| 8.00% | Basic and Advanced Cryptography | 3, 12, 13, 14, 15, 16 |
| 10.00% | Wireless and Mobile Security | 8, 10, 11, 12, 13, 14, 15, 16 |
| 6.00% | Risk Mitigation | 1, 2, 3, 4, 9, 11, 12, 13, 16 |
| **Lab** (must total 100%) | | |
| 7.00% | Perform lab(s) on Attacks and malicious code | 1 |
| 7.00% | Perform lab(s) on E-Mail | 5, 6, 14 |
| 6.00% | Perform lab(s) on Wireless and instant messaging | 8 |
| 6.00% | Perform lab(s) on Security related devices | 9, 10, 12 |
| 6.00% | Perform lab(s) on Media and medium | 10 |
| 6.00% | Perform lab(s) on Network security topologies | 11, 15 |
| 6.00% | Perform lab(s) on Physical security | 9, 11, 12, 15 |
| 6.00% | Perform lab(s) on Disaster recovery and business continuity | 7, 16 |
| 8.00% | Perform lab(s) on Security overview | 1, 4, 13, 14 |
| 8.00% | Perform lab(s) on Authentication | 2, 7, 14 |
| 7.00% | Perform lab(s) on Web security | 5, 6, 13 |
| 6.00% | Perform lab(s) on Directory and file transfer services | 6 |
| 7.00% | Perform lab(s) on Security baselines | 9, 10, 12, 16 |
| 8.00% | Perform lab(s) Crytography | 3, 4 |
| | | |

| | | |
|---|---|---|
| 6.00% | Perform lab(s) Intrusion detection | 1, 12 |

## IV. TYPICAL ASSIGNMENTS

### A. Writing assignments

| Writing assignments are required. Possible assignments may include, but are not limited to: | |
|---|---|
| 1 | summarize and write an analysis of newspaper and journal articles on recent security topics such as hackers stealing confidential information. |
| 2 | write an analysis paper on how security encryption compare between symmetric and asymmetric encryption methods. |

### B. Appropriate outside assignments

| Appropriate outside assignments are required. Possible assignments may include, but are not limited to: | |
|---|---|
| 1 | conduct research by comparing antivirus applications from common providers such as Kaspersky, Norton, Mcafee, Eset, etc. |
| 2 | Research common root kit viruses and malware such as adware, bots, bugs, ransomware, spyware, trojan house, worm, etc. |

### C. Critical thinking assignments

| Critical thinking assignments are required. Possible assignments may include, but are not limited to: | |
|---|---|
| 1 | present a security confidentiality policy and explain the need for protecting customer confidentially. |
| 2 | present a security law or regulation and what protection that law provides such as the Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act, and other popular security laws or regulations. |

## 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) Online materials
Assigned Internet research

□ Optional Field Trips

□ Required Field Trips

## VI. METHODS OF EVALUATION

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

□ Essay Exam ☒ Classroom Discussion ☒ Skill Demonstration

| | | |
|---|---|---|
| ☒ Problem Solving Exam | ☒ Reports/Papers/ Journals | □ Participation |
| ☒ Objective Exams | ☒ Projects | ☒ Other (specify) |

Assess technical security skills in a lab environment.

## VII. REPRESENTATIVE TEXTS AND OTHER COURSE MATERIALS

Ciampa, Mark . CompTIA Security+ Guide to Network Security Fundamentals, Deluxe Study Guide. 6th ed. Course Technology, 2017.

Stallings, William. Network Security Essentials: Applications and Standards. 6th ed. Pearson, 2016.

## VIII. STUDENT MATERIALS FEES

☒ No □ Yes

## IX. PARALLEL COURSES

| *College* | *Course Number* | *Course Title* | *Units* |
|---|---|---|---|
| Cal State San Bernardino | INFO 275 | Information Networking and Security | 4 |
| Cabrillo College | CIS 75 | Fundamentals of Computer Security | 3 |
| Mendocino College | CSC 118 | Introduction to Information Systems Security | 3 |

## X. MINIMUM QUALIFICATIONS

**Courses in Disciplines in which Masters Degrees are not expected:**
Associate Degree and 6 years networking experience and CCNA or MCSA certificate, 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:
Research, using the Library's print and online resources, for a paper which discusses a basic concept of security that deals with either confidentiality and its remediation method, integrity and its remediation method, or authentication and its remediation method.

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 M82: 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, evaluate projects, and solve technical security problem scenarios.
3. Information: the students will acquire and use information through a variety of assignments, security tools, and computer software applications used in securing computer systems.
4. Systems: the students will employ a variety of computer security tools to complete projects or assess computer security problems.
5. Technology: the students will use modern technology to acquire the skills needed to prepare for a career.

The course also addresses the SCANS skills and personal qualities:

1. Basic Skills: the students will read, perform computer mathematic operations, listen and speak for weekly assignments and participate in classroom discussions.
2. Thinking Skills: the students will think creatively, make decisions, solve security problems and provide reasonable problem solving skills after satisfactorily completing this course.
3. Personal Qualities: the students will be required to display responsibility, self-management, integrity, and honesty throughout course work and classroom exercises.

## 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.

   The instructor will be available online and will monitor the Distance Learning online course.  The instructor will use the available tools in the course management system (CMS) for two-way student/instructor communication. Instructor will use the CMS tools in order to provide assessments such as assignments and quizzes.

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

   Discussion boards.  Other tools, online and PC resident, and forums will be used so that students can practice their skills as it applies to the course material. Through the course management system (CMS), materials will be made available online for download.  Assessments for measuring understanding and student performance feedback will be made available through the CMS tools. Assignments, labs, and discussions will be available online.

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

   All security topics are available for research online and align with CompTia Security+ curriculum.  Videos and online discussion boards.

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

   Quizzes, Homework, Labs, and Exams.

## XVI. GENERAL EDUCATION COURSE OUTLINE ADDENDUM

CNSE M82: Not Applicable

## XVII. STUDENT MATERIALS FEE ADDENDUM

CNSE M82: Not Applicable

## XVIII. REPEATABILITY JUSTIFICATION TITLE 5, SECTION 55041

CNSE M82: Not Applicable

## XIX. CURRICULUM APPROVAL

Course Information:

Discipline:
COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

Discipline Code and Number: CNSE M82

Course Revision Category: Substantial Course Revision

Course Proposed By:

Originating Faculty Edmond Garcia 08/25/2017

Faculty Peer: Edmond Garcia 08/25/2017

Curriculum Rep: __________

Department Chair: Navreet Sumal 09/02/2017

Division Dean: Howard Davis 08/28/2017

Approved By:

Curriculum Chair: Jerry Mansfield 10/13/2017

Executive Vice President: Julius Sokenu 10/13/2017

Articulation Officer: Letrisha Mai 09/21/2017

Librarian: Mary LaBarge 09/20/2017

Implementation Term and Year: Fall 2018

Approval Dates:

Approved by Moorpark College Curriculum Committee: 10/03/2017

Approved by Board of Trustees (if applicable): 12/12/2017

Approved by State (if applicable): 01/12/2018