I. CATALOG INFORMATION

A. Discipline: COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

B. Subject Code and Number: CNSE M100

C. Course Title: Cybersecurity Analysis

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: [X] 1 [ ] 2 [ ] 3 [ ] 4 time(s) for credit

H. Is the course co-designated (same as) another course: No [X] Yes [ ]
If YES, designate course Subject Code & Number: _____

I. Course Description:

Provides training for security analysts in areas of vulnerability and threat analysis. Includes instruction in the use of threat detection tool sets to perform security architecture analysis, and interpret results to mitigate vulnerabilities. Covers how to best handle security incidents.

J. Entrance Skills

*Prerequisite: No [X] Yes [ ] Course(s)

_____

*Corequisite: No [X] Yes [ ] Course(s)

_____

Limitation on Enrollment: No [X] Yes [ ]

_____

Recommended Preparation: No [ ] Yes [X] Course(s)
CNSE M82

Other: No [X] Yes [ ]

_____

K. Other Catalog Information:

This course helps prepare students to pass Cybersecurity Analyst Exam from CompTIA. This course is best taken after Security Plus and before Certified Ethical Hacker. See Comptia.org for more details.

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	analyze the results of network and environmental reconnaissance.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
2	recommend and implement response and countermeasures.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
3	apply best practices in securing a corporate environment.	Quizzes Midterms Final Exam Classroom project work demonstrating competency in this area
4	implement an Information Security Vulnerability Management process.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
5	analyze scan output and identify common vulnerabilities.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
		Quizzes Midterms Final exam

6	identify incident impact and assemble a forensics toolkit.	Classroom project work demonstrating competency in this area
7	implement the incident response process.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
8	perform incident recovery and post-incident response.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
9	develop frameworks, policies, controls and procedures as they apply to security.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
10	perform security remediation.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
11	apply application security best practices.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area
12	utilize cybersecurity tools and technologies.	Quizzes Midterms Final exam Classroom project work demonstrating competency in this area

III. COURSE CONTENT

		Learning

Estimated %	Topic	Outcomes
Lecture (must total 100%)		
7.00%	A. Applying Reconnaissance 1. Procedures and common tasks 2. Variables 3. Tools	1, 2
7.00%	B. Analyzing Results 1. Point-in-time data analysis 2. Data correlation 3. Data output 4. Tools	1, 2
7.00%	C. Response and Countermeasures 1. Network segmentation 2. Honeypot 3. Security endpoints 4. Policies 5. Access controls lists 6. Hardening 7. Network access control	2, 3, 4, 5
7.00%	D. Securing Corporate Enterprise 1. Penetration testing 2. Reverse engineering 3. Training 4. Risk evaluation	1, 2, 3, 5, 6
7.00%	E. Information Security Vulnerability Management 1. Requirements 2. Scanning criteria and frequency 3. Tools 4. Reports and documentation 5. Remediation 6. Monitoring	1, 2, 3, 4, 5
7.00%	F. Scan Output and Identifying Common Vulnerabilities 1. Interpreting results 2. Common vulnerabilities and exposures: servers, endpoints, network infrastructure,network appliances, mobile devices, virtual private networks, industrial control systems	3, 4, 5, 6
7.00%	G. Incident Impact and Forensic Toolkit 1. Threat classification 2. Incident severity and prioritization 3. Types of data 4. Forensics kits and forensics workstation 5. Investigation suite	3, 4, 5, 6, 9, 10, 11, 12
7.00%	H. Incident Response Process 1. Stakeholders 2. Communication process: trusted parties, regulatory requirements, release of information, methods of communications 3. Role-based responsibilities 4. Understanding common symptoms to support best course of action	3, 4, 8, 9
7.00%	I. Incident Recovery and Post-Incident Response 1. Containment 2. Eradication 3. Validation 4. Corrective actions	3, 4, 5, 7, 8, 9, 10

	5. Incident summary report	
7.00%	J. Frameworks, Policies, Controls, and Procedures 1. Regulatory compliance 2. Frameworks: National Institute of Standards and Technology, International Standards Organization, etc. 3. Policies 4. Controls 5. Procedures 6. Verification and quality control: audits, evaluations, assessments, certification	3, 4, 7, 8, 9
7.00%	K. Remediation 1. Authentication 2. Identities 3. Repositories 4. Federation and single sign-on 5. Exploits	9, 10, 11, 12
7.00%	L. Security Architecture and Compensating Controls 1. Data analysis 2. Manual review 3. Defense in depth	4, 5, 6, 7, 8, 9, 10, 11, 12
16.00%	M. Best Practices and Security Tools 1. Intruder detection systems 2. Intruder prevention systems 3. Firewalls 4. Antivirus 5. Anti-malware 6. Web proxy 7. Collective tools 8. Scanning tools 9. Packet capture 10. Internet protocol utilities 11. Command line utilities 12. Analytical tools 13. Exploit tools 14. Forensics tools 15. Hashing 16. Password cracking 17. Imaging	3, 6, 8, 9, 10, 11, 12
Lab (must total 100%)		
8.00%	Working with Wireshark for Packet Analysis	1, 2, 3, 5
16.00%	Nmap for network mapping, fingerprinting, port scanning, and service discovery	1, 2, 3, 4, 5
8.00%	Tracert, netstat, nslookup, ipconfig, ping and other network utilities	3, 4, 5, 6
8.00%	VMware, virtual box, virtual machines	2, 3, 5, 6, 11, 12
8.00%	Firewalls	1, 2, 3, 5, 9, 10, 11, 12
8.00%	Linux and Windows Security tools such as Nessus, Kali Linux, Metasploit, Snort, Backtrack, Tcpdump and other modern security products.	1, 2, 3, 5, 6, 12
16.00%	Forensics Tool Kits	1, 3, 4, 5, 10, 11, 12

4.00%	Logging and Monitoring Tools such as Nessus, Kali Linux, Metasploit, Snort, Backtrack, Tcpdump and other modern security products.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
8.00%	Packet Tracer for Access-Lists	2, 3, 5, 9, 10, 12
8.00%	Switching and Security	3, 5, 9, 10, 12
8.00%	Linux and Windows Scripting	2, 3, 5, 6, 9, 10, 11, 12

IV. TYPICAL ASSIGNMENTS

A. Writing assignments

Writing assignments are required. Possible assignments may include, but are not limited to:	
1	write about solutions and best practices that contribute to security remediation.
2	develop written documentation that supports an organization's security policy.
3	provide documentation in support of an incident response.

B. Appropriate outside assignments

Appropriate outside assignments are required. Possible assignments may include, but are not limited to:	
1	research topics related to new security solutions, new security problems, and offer solutions for remediation to circumvent security challenges.
2	research new security assessment tools and how they provide modern solutions in system and network protection.

C. Critical thinking assignments

Critical thinking assignments are required. Possible assignments may include, but are not limited to:	
1	discuss evidence collected from logs and monitoring tools and interpret what may have happened and how to remediate.
2	use forensics tool kits and network security tools to assess security posture of a given environment and provide solutions for securing business environments.

V. METHODS OF INSTRUCTION

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

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

[X] Lecture/Discussion

[X] Laboratory/Activity

[X] Other (Specify)
Use of an online system as recommended by South Central Coast Regional consortium in order to increase student online lab access to 24/7.

☐ 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)

Performance-based lab assessment.

VII. REPRESENTATIVE TEXTS AND OTHER COURSE MATERIALS

McMillan, Troy. CompTIA Cybersecurity Analyst (CSA+) Certification Guide. Pearson, 2017.

Maymi, Fernando, and Brent Chapman. CompTIA CySA+ Cybersecurity Analyst Certification; All-in-One Exam Guide. McGraw-Hill Education, 2017.

VIII. STUDENT MATERIALS FEES

☒ No ☐ Yes

IX. PARALLEL COURSES

College	*Course Number*	*Course Title*	*Units*
City College of Chicago	COMPSFI 214	Information Security Systems Analysis	4
North Virginia Community College	ITN 266	NETWORK SECURITY LAYERS	3
Commmunity College of Philadelphia	CIS 261	Cyber Investigation	4
Tidewater Community College	ITN 261	Network Attacks, Computer Crime and Hacking	4

X. MINIMUM QUALIFICATIONS

Courses in Disciplines in which Masters Degrees are not expected:
Any Bachelor's degree and two years professional experience, or any associate degree and six years of professional experience, or 3 years professional experience in security with one security certification.

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 [X] 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: [X] 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: [X] No: [ ]

2. If YES do you recommend this course for inclusion on the CSU General Education list?
   Yes: [ ] No: [X] 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: [X]

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

   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, on topics such as modern security tools, modern threats and vulnerabilities, and data analysis.

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

YES: [X] NO: [ ]

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

XIII. PREREQUISITE AND/OR COREQUISITE JUSTIFICATION

CNSE M100: 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 know how to use security tools in performing network and application vulnerability and threat analysis.
2. Interpersonal: the students will be required to participate in group-based security assessments.
3. Information: the students will learn to document threats and vulnerability discoveries and prepare mitigation recommendations based on security best practices principles.
4. Systems: the students will learn about the use of various security tools in assessing computer systems and networks.
5. Technology: the students will learn to use security applications to perform security audits.

The course also addresses the SCANS skills and personal qualities:

1. Basic Skills: the students will have reading and writing assignments, perform mathematical or binary operations or use hexadecimal notation, and listen, speak, or complete assignments and exercises on a weekly basis.
2. Thinking Skills: the students will develop critical thinking skills through project analysis and problem solving.
3. Personal Qualities: the students will learn about responsibility, time management, integrity, and teamwork through assigned individual and group projects.

XV. DISTANCE LEARNING COURSE OUTLINE ADDENDUM

1. Mode of Delivery

[X] Online (course will be delivered 100% online)

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

[ ]

[X] 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

[X] Other Use of Netlabs.

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 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.

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; students may engage in internet; 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; illustrations provided by curriculum vendor; links to online resources that may include videos, quizzes, text explanations and extensions, and primary documents; homework assignments; security assessment analysis.

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

   Students may take objective and performance based exams in an online teaching environment. Students may be required to do the following assignments: complete reflective analysis assignments focused on application of

course content; develop, implement, and evaluate security assessment projects; complete regular online quizzes; complete performance assignments related to key course concepts; participate in online discussion forums.

XVI. GENERAL EDUCATION COURSE OUTLINE ADDENDUM

CNSE M100: Not Applicable

XVII. STUDENT MATERIALS FEE ADDENDUM

CNSE M100: Not Applicable

XVIII. REPEATABILITY JUSTIFICATION TITLE 5, SECTION 55041

CNSE M100: Not Applicable

XIX. CURRICULUM APPROVAL

Course Information:

Discipline:
COMPUTER NETWORKING SYSTEMS ENGINEERING (CNSE)

Discipline Code and Number: CNSE M100

Course Revision Category: New Course

Course Proposed By:

Originating Faculty Edmond Garcia 11/05/2017

Faculty Peer: Edmond Garcia 11/05/2017

Curriculum Rep: _____

Department Chair: Navreet Sumal 11/06/2017

Division Dean: Howard Davis 11/06/2017

Approved By:

Curriculum Chair: Jerry Mansfield 12/07/2018

Executive Vice President: _____

Articulation Officer: Jodi Dickey 02/28/2018

Librarian: Mary LaBarge 02/25/2018

Implementation Term and Year: Fall 2019

Approval Dates:

Approved by Moorpark College Curriculum Committee: 11/20/2018

Approved by Board of Trustees (if applicable): 02/19/2019

Approved by State (if applicable): 02/25/2019