ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2201 Ethical Hacking I

Date: Fall 2020

Credit Hours: 3

Prerequisite(s): None

Delivery Method:		
	☒ **Lecture**	**3 Contact Hours (1 contact = 1 credit hour)**
	☐ **Seminar**	**0 Contact Hours (1 contact = 1 credit hour)**
	☒ **Lab**	**2 Contact Hours (2-3 contact = 1 credit hour)**
	☐ **Clinical**	**0 Contact Hours (3 contact = 1 credit hour)**
	☐ **Online**	
	☐ **Blended**	

Offered: ☒ **Fall** ☐ **Spring** ☐ **Summer**

IAI Equivalent –***Only for Transfer Courses***-go to *http://www.itransfer.org*:

CATALOG DESCRIPTION:
This is the first of two Ethical Hacking courses that focus on EC-Council's Certified Ethical Hacker (C|EH v10) training and certification program. Certified Ethical Hacking skills have become a core skillset and a cyber staple within Cybersecurity and Information Technology. This course will provide you with the tools and techniques used by hackers and information security professionals alike to gain information, attack and detect malicious activity. This course in conjunction with Ethical Hacking 2 is designed to provide you with the knowledge necessary to sit for EC-Council's Certified Ethical Hacker exam.

GENERAL EDUCATION GOALS ADDRESSED

[See last page for Course Competency/Assessment Methods Matrix.]

Upon completion of the course, the student will be able:

[Choose up to three goals that will be formally assessed in this course.]

☒ To apply analytical and problem solving skills to personal, social, and professional issues and situations.
☐ To communicate successfully, both orally and in writing, to a variety of audiences.
☐ To construct a critical awareness of and appreciation for diversity.
☒ To understand and use technology effectively and to understand its impact on the individual and society.
☐ To develop interpersonal capacity.
☒ To recognize what it means to act ethically and responsibly as an individual and as a member of society.
☐ To recognize what it means to develop and maintain a healthy lifestyle in terms of mind, body, and spirit.
☐ To connect learning to life.

EXPECTED LEARNING OUTCOMES AND RELATED COMPETENCIES:

[Outcomes related to course specific goals. See last page for more information.]

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

1. Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.
2. Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing security of various components of information.
3. Examine different vulnerabilities, threats and attacks to information systems and recommend the countermeasures.
4. Assess various network security techniques and tools and implement appropriate level of information security controls based on evidence, information and research.

Outcome 1 - Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.

Competency 1.1 - Explain why a systematic approach is necessary for a successful attack
Competency 1.2 – Understand the significance of competitive intelligence gathering for an organization in succeeding in this field

Outcome 2 - Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing security of various components of information.

Competency 2.1 - Successfully footprint an organization and information system as well as recommend countermeasures to vulnerabilities found.
Competency 2.2 - Perform reconnaissance on a target
Competency 2.3 - Obtain a blueprint of the security profile of a target organization
Competency 2.4 - Employ various vulnerability scanning techniques to perform enumeration on a network.

Outcome 3 - Examine different vulnerabilities, threats and attacks to information systems and recommend the countermeasures.

Competency 3.1 – Effectively scan a Network for vulnerabilities
Competency 3.2 - Monitor systems remotely and extract hidden files and passwords
Competency 3.3 - Detect Trojan and backdoor attacks
Competency 3.4 – Analyze virus infection mechanisms (attack and detect)
Competency 3.5 - Effectively sniff a network and perform packet analysis for attacks on a network
Competency 3.6 - Perform a DDoS attack
Competency 3.7 – Take control of a computer remotely
Competency 3.8 - Clone a website and perform/protect the network from phishing attacks

Outcome 4 - Assess various network security techniques and tools and implement appropriate level of information security controls based on evidence, information and research.

Competency 4.1 - Discuss countermeasures that should be performed to prevent systems from various threats
Competency 4.2 – Understand different types of Steganography methods used for hiding confidential data
Competency 4.3 - Capture traffic and collect data from any network topology
Competency 4.4 - Perform a technical security assessment

MAPPING LEARNING OUTCOMES TO GENERAL EDUCATION GOALS

[For each of the goals selected above, indicate which outcomes align with the goal.]

Goals	Outcomes
First Goal	
To apply analytical and problem-solving skills to personal, social, and professional issues and situations.	1. Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements. 2. Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing security of various components of information.
Second Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	3. Examine different vulnerabilities, threats and attacks to information systems and recommend the countermeasures.
Third Goal	
To recognize what it means to act ethically and	4. Assess various network security techniques and tools and implement appropriate level of

responsibly as an individual and as a member of society.	information security controls based on evidence, information and research.

COURSE TOPICS AND CONTENT REQUIREMENTS:

- Intro to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service

INSTRUCTIONAL METHODS:

- Lecture
- EC-Council iLabs
- Case Studies
- Group work/discussions

INSTRUCTIONAL MATERIALS:

EC-Council eBook CEH v10 (from EC-Council Academia Site
Ethical Hacking Concepts and Methodology – Volume 1
Attack Vectors and Countermeasures – Volume 2

EC-Council iLabs – Accessed on EC-Council Site
iLabs Modules: 1, 2, 3, 4, 5, 6, 7, 8, 9, & 10

STUDENT REQUIREMENTS AND METHODS OF EVALUATION:

A= 90-100
B= 80-89
C= 70-79
D= 60-69
F= 0-59

OTHER REFERENCES

Case Studies
White Paper

Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																																
For each competency/outcome place an "X" below the method of assessment to be used.	**Assessment of Student Learning**	Article Review	Case Studies	Group Projects	Lab Work	Oral Presentations	Pre-Post Tests	Quizzes	Written Exams	Artifact Self Reflection of Growth	Capstone Projects	Comprehensive Written Exit Exam	Course Embedded Questions	Multi-Media Projects	Observation	Writing Samples	Portfolio Evaluation	Real World Projects	Reflective Journals	Applied Application (skills) Test	Oral Exit Interviews	Accreditation Reviews/Reports	Advisory Council Feedback	Employer Surveys	Graduate Surveys	Internship/Practicum /Site Supervisor Evaluation	Licensing Exam	In Class Feedback	Simulation	Interview	Written Report	Assignment
Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.	**Direct/ Indirect**	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
1. Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.			X		X			X					X					X														X
1.1. Explain why a systematic approach is necessary for a successful attack.			X		X			X					X					X														X
1.2. Understand the significance of competitive intelligence gathering for an organization in succeeding in this field			X		X			X					X					X														X

2. Analyze different phases of hacking and recommend the strategy to use ethical hacking for assessing security of various components of information.			X		X			X					X					X													X
2.1. Successfully footprint an organization and information system as well as recommend countermeasures to vulnerabilities found.			X		X			X					X					X													X
2.2. Perform reconnaissance on a target			X		X			X					X					X													X
2.3. Obtain a blueprint of the security profile of a target organization			X		X			X					X					X													X
3. Examine different vulnerabilities, threats and attacks to information systems and recommend the countermeasures.			X		X			X					X					X													X
3.1 Effectively scan a Network for vulnerabilities.			X		X			X					X					X													X
3.2. Monitor systems remotely and extract hidden files.			X		X			X					X					X													X
3.3. Detect Trojan and backdoor attacks.			X		X			X					X					X													X
3.4. Analyze virus infection mechanisms (attack and detect).			X		X			X					X					X													X
3.5. Effectively sniff a network and perform packet analysis for attacks on a network.			X		X			X					X					X													X
3.6. Perform a DDoS attack			X		X			X					X					X													X
3.7. Take control of a computer remotely.			X		X			X					X					X													X
3.8. Clone a website and perform/protect the network from phishing attack.			X		X			X					X					X													X

4. Assess various network security techniques and tools and implement appropriate level of information security controls based on evidence, information and research.			X		X			X					X					X													X
4.1. Discuss countermeasures that should be performed to prevent systems from various threats.			X		X			X					X					X													X
4.2 Understand different types of Steganography methods used for hiding confidential data.			X		X			X					X					X													X
4.b. Capture traffic and collect data from any network topology.			X		X			X					X					X													X
4.c. Perform a technical security assessment.			X		X			X					X					X													X