ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2201 Ethical Hacking I

Date: Fall 2021

Credit Hours: 3

Prerequisite(s): Basic Computer Knowledge

Delivery Method:

☒ **Lecture**	**2 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**		
☒ **VCM**		

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

CATALOG DESCRIPTION and IAI NUMBER (if applicable):
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.

ACCREDITATION STATEMENTS AND COURSE NOTES:
None

COURSE TOPICS AND CONTENT REQUIREMENTS:
1. Overview of Ethical Hacking
2. Reconnaissance
3. Scanning
4. Vulnerability Analysis
5. System Hacking
6. Malware Threats
7. Social Engineering
8. Denial-of-Service
9. Wireless Networks

INSTRUCTIONAL METHODS:
1. Lecture
2. Discussion
3. Readings
4. Case Studies
5. Hands-On Ethical Hacking Labs

EVALUATION OF STUDENT ACHIEVEMENT:
Students must:
1. Participate in class discussions or demonstrate by work completed the recorded videos of class were reviewed
2. Complete readings, assignments, quizzes, exams, hands-on EC-Council labs, and other assignments given at the instructor's discretion
3. Ask questions about any misunderstood area either in class, during office hours, or of the tutor.

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

INSTRUCTIONAL MATERIALS:
Textbooks
Textbooks used in Ethical Hacking I are at the discretion of full-time faculty.
Part-time faculty members are to use the textbook designated for Ethical Hacking I by the Program Coordinator for Cybersecurity and the Dean of Workforce Development.

Resources
EC-Council eBook CEH (current version)
- Ethical Hacking Concepts and Methodology – Volume 1
- Ethical Hacking Attack Vectors and Countermeasures – Volume 2
- EC-Council iLabs for Volume 1 & 2
- Case Studies

Computer Applications:
1. Word Processing software
2. Web Browser:
    a. Vital Source
    b. EC-Council iLab site
3. Online Course Management Software
4. IVCC email account

Other:

1. Audio/video resources

LEARNING OUTCOMES AND GOALS:

Institutional Learning Outcomes

☐ ILO 1: Communication – to communicate effectively;

☒ ILO 2: Inquiry – to apply critical, logical, creative, aesthetic, or quantitative analytical reasoning to formulate a judgement or conclusion;

☒ ILO 3: Social Consciousness – to understand what it means to be a socially conscious person, locally and globally;

☐ ILO 4: Responsibility – to recognize how personal choices affect self and society.

Course Outcomes and Competencies

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.

Competency 2.5: Explain different phases of advanced persistent threat lifecycle and analyze its characteristics.

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.