ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2205 Ethical Hacking II

Date: Fall 2021

Credit Hours: 3

Prerequisite(s): CSC 2201 Ethical Hacking I

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 second of two Ethical Hacking courses that focus on EC-Council's Certified Ethical Hacker (C|EH v10) training and certification program. This course will provide you with the tools and techniques used by hackers and information security professionals alike to break into any computer system, bypass controls and hijack sessions. This course in conjunction with Ethical Hacking I 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. Session Hijacking
2. Evading Security Appliances
3. Hacking Web Servers & Applications
4. SQL Injection
5. Hacking Wireless Networks
6. Hacking Mobile Platforms
7. IoT Hacking
8. Cloud Computing
9. Cryptography

INSTRUCTIONAL METHODS:

1. Lecture
2. Discussion
3. Readings
4. Case Studies
5. Student Presentations
6. 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, presentations, 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 II are at the discretion of full-time faculty.
Part-time faculty members are to use the textbook designated for Ethical Hacking II by the Program Coordinator for Cybersecurity and the Dean of Workforce Development.

Resources

EC-Council eBook CEH (current version)

- Ethical Hacking Web Attacks and Defense – Volume 3
- Ethical Hacking Infrastructure Security Threats & Controls – Volume 4
- EC-Council iLabs for Volume 3 & 4
- Case Studies

Computer Applications:

1. Word Processing software
2. Presentation software (PPTX/Google Slides)
3. Web Browser:
   a. Vital Source
   b. EC-Council iLab site
4. Online Course Management Software
5. 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: Compare and contrast different hacking techniques and analyze the legal implications
Competency 1.1: Use various tools to hijack a session
Competency 1:2: Apply different tools to intercept web traffic
Competency 1.3: Effectively bypass security appliances

Outcome 2: Examine different vulnerabilities, threats and attacks to information systems and recommend the counter measures
Competency 2.1: Understanding honeypots and their role in safeguarding the network.
Competency 2.2: Explain the Consequences of SQL injection attacks
Competency 2.3: Understand effective techniques to hack wireless networks
Competency 2.4: Understand the threats and attacks on mobile and IoT devices
Competency 2.5: Explain the threats and vulnerabilities associated with Cloud Computing

Outcome 3: Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information.
Competency 3.1: Understand explain various cryptographic techniques and design
Competency 3.2: Explain Cloud service design strategies
Competency 3.3: Apply and understand the benefits of Disk Encryption

Outcome 4: Compare and contrast various network security assessment and hacking tools.
Competency 4.1: Take over a user account through session hijacking

Outcome 5: Assess various network security techniques and tools and implement appropriate level of information security controls based on evidence, information, and research.
Competency 5.1: Understand through research and analysis of various tools, vulnerabilities, techniques the strategies and legal implications of their use.
Competency 5.2: Present research on a breach of network security, and the method used to gain access