ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2205 Ethical Hacking II

Date: Fall 2019

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**	

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

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

CATALOG DESCRIPTION:
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.

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. Compare and contrast different hacking techniques and analyze the legal implications
2. Examine different vulnerabilities, threats and attacks to information systems and recommend the counter measures
3. Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information.
4. Compare and contrast various network security assessment and hacking tools.
5. Assess various network security techniques and tools and implement appropriate level of information security controls based on evidence, information and research.

Outcome 1 - Compare and contrast different hacking techniques and analyze the legal implications

Competency 1.1 – Bypassing a firewall
Competency 1.2 – Web Attacks and hijacks
Competency 1.3 – Detecting intrusions in a network

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 – Consequences of SQL injection attacks
Competency 2.3 – Hacking wireless networks
Competency 2.4 – Hacking mobile android devices
Competency 2.5 – Bypassing Cloud AV

Outcome 3 - Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information.

Competency 3.1 – Securing with Open SSL Encryption
Competency 3.2 – Cloud services
Competency 3.3 – 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.

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. Compare and contrast different hacking techniques and analyze the legal implications.
Second Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	2. Examine different vulnerabilities, threats and attacks to information systems and recommend the counter measures 3. Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information.
Third Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	4. Examine different vulnerabilities, threats and attacks to information systems and recommend the counter measures 5. Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information.

COURSE TOPICS AND CONTENT REQUIREMENTS:

- Session Hijacking
- Evading IDS, Firewalls, and Honeypot
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

INSTRUCTIONAL METHODS:

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

INSTRUCTIONAL MATERIALS:

EC-Council eBook CEH v10 (from EC-Council Academia Site
Web Attacks and Defense – Volume 3
Infrastructure Security Threats and Controls – Volume 4

EC-Council iLabs – Accessed on EC-Council Site
iLabs Modules: 11, 12, 13, 14,15, 16, 17, 18, 19, 20

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. Compare and contrast different hacking techniques and analyze the legal implications			X		X			X					X					X														X
1.1 Bypassing a firewall			X		X			X					X					X														X
1.2 Web Attacks and hijacks			X		X			X					X					X														X
1.3 Detecting intrusions in a network			X		X			X					X					X														X
2. Examine different vulnerabilities, threats and attacks to information systems and recommend the counter measures			X		X			X					X					X														X

2.1 Understanding honeypots and their role in safeguarding the network			X		X			X					X					X												X
2.2 Consequences of SQL injection attacks			X		X			X					X					X												X
2.3 Hacking wireless networks			X		X			X					X					X												X
2.4 Hacking mobile android devices			X		X			X					X					X												X
2.5 Bypassing Cloud AV			X		X			X					X					X												X
3. Analyze cryptography algorithms and encryption techniques, and design implementation strategies for securing information			X		X			X					X					X												X
3.1 Securing with Open SSL Encryption			X		X			X					X					X												X
3.2 Cloud services			X		X			X					X					X												X
3.3 Disk Encryption			X		X			X					X					X												X
4. Compare and contrast various network security assessment and hacking tools			X		X			X					X					X												X
4.1 Take over a user account through session hijacking			X		X			X					X					X												X
5. 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

5.1 Understand through research and analysis of various tools, vulnerabilities, techniques the strategies and legal implications of their use			X		X			X					X					X													X