



ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2202 Cybersecurity Scripting

Date: August 28, 2018

Credit Hours: 3

Prerequisite(s): CSO 2200, CSN 1225

Delivery Method:

<input checked="" type="checkbox"/> Lecture	2 Contact Hours (1 contact = 1 credit hour)
<input type="checkbox"/> Seminar	0 Contact Hours (1 contact = 1 credit hour)
<input checked="" type="checkbox"/> Lab	2 Contact Hours (2-3 contact = 1 credit hour)
<input type="checkbox"/> Clinical	0 Contact Hours (3 contact = 1 credit hour)
<input type="checkbox"/> Online	
<input type="checkbox"/> Blended	

Offered: Fall Spring Summer

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

CATALOG DESCRIPTION:

This course teaches students to identify potential vulnerabilities related to scripting and to understand script writing using Python and other scripting languages. The students will create scripts that monitor network traffic, analyze files and automate vulnerability assessment and exploitation. Lecture 2 hours; lab, 2 hours.

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 appreciate 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. Learn to install a Python IDE and write simple scripts.
2. Write network traffic scripts.
3. Write scripts for wireless penetration.
4. Write scripts to do web-based recon.
5. Write scripts for antiviruses.

Outcome 1 – Upon completion of the course, the student will learn to install a Python IDE and write simple scripts.

Competency 1.1 – The student will learn about the basics of the Python language and when it should be used.

Competency 1.2 – The student will write programs using Python

Competency 1.3 – The student will compare Python to other scripting languages to see which ones fit the desired task.

Outcome 2 – Upon completion of the course, the student will be able to write network traffic scripts.

Competency 2.1 – The student will write Python programs to script attacks for penetration testing including port scanning, SSH penetration, and mass-compromising via FTP

Competency 2.2 – The student will write scripts that represent an exploit.

Competency 2.3 – The student will utilize Python for digital forensic investigations

Competency 2.4 – The student will use Python for network traffic analysis

Outcome 3 – Upon completion of the course, the student will be able to write scripts for wireless penetration

Competency 3.1 – The student will write scripts to break wireless and Bluetooth devices

Competency 3.2 – The student will write scripts to combat wireless and Bluetooth device hacks

Outcome 4 – Upon completion of the course, the student will write scripts to do web-based recon.

Competency 4.1 – The student will write scripts to scrape websites for information.

Competency 4.2 – The student will write scripts to scrape popular social media sites for information

Competency 4.3 – The student will write scripts to spear-phish email.

Outcome 5 - Upon completion of the course, the student will be able to write scripts for antiviruses.

Competency 5.1 – The student will write malware that evades antivirus systems.

Competency 5.2 – The student will write scripts to combat malware that evades antivirus systems.

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	<ol style="list-style-type: none"> 1. Learn to install a Python IDE and write simple scripts. 2. Write network traffic scripts. 3. Write scripts for wireless penetration. 4. Write scripts to do web-based recon. 5. Write scripts for antiviruses.
Second Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	<ol style="list-style-type: none"> 1. Learn to install a Python IDE and write simple scripts. 2. Write network traffic scripts. 3. Write scripts for wireless penetration. 4. Write scripts to do web-based recon. 5. Write scripts for antiviruses.

COURSE TOPICS AND CONTENT REQUIREMENTS:

- Learning the Python programming language
- Penetration Testing with Python
- Forensic Investigations with Python
- Network Traffic Analysis with Python
- Wireless Penetration Testing with Python
- Web Recon and Hacking with Python
- Antivirus Evasion with Python

INSTRUCTIONAL METHODS:

- Lecture, online discussion threads, case studies, group work/discussions

INSTRUCTIONAL MATERIALS:

Violent Python by T.J. O'Connor

Publisher: Syngress

ISBN: 978-1597499576

STUDENT REQUIREMENTS AND METHODS OF EVALUATION:

A= 90-100

B= 80-89

C= 70-79

D= 60-69

F= 0-59

OTHER REFERENCES

Black Hat Python: Python Programming for Hackers and Pentesters by Just Seitz

Publisher: No Starch Press

ISBN: 978-1593275900

Hacking with Python: The complete Beginner's Guide to Learning Ethical Hacking with Python along with Practical Examples by Miles Price

Publisher: CreateSpace Independent Publishing Platform

ISBN: 978-1981832255

Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																															
<p>For each competency/outcome place an "X" below the method of assessment to be used.</p>	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
<p>Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.</p>	Direct/	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
<p>Competency 1.1 – The student will learn about the basics of the Python language and when it should be used.</p>								X	X																		X				X	
<p>Competency 1.2 – The student will write programs using Python.</p>				X			X	X																			X				X	
<p>Competency 1.3 – The student will compare Python to other scripting languages to see which ones fit the desired task.</p>							X	X																			X					

Competency 2.1 – The student will write Python programs to script attacks for penetration testing including port scanning, SSH penetration, and mass-compromising via FTP.				X			X	X																					X					X
Competency 2.2 – The student will write scripts that represent an exploit.				X			X	X																					X					X
Competency 2.3 – The student will utilize Python for digital forensic investigations.				X			X	X																					X					X
Competency 2.4 – The student will use Python for network traffic analysis.				X			X	X																					X					X
Competency 3.1 – The student will write scripts to break wireless and Bluetooth devices.				X			X	X																					X					X
Competency 3.2 – The student will write scripts to combat wireless and Bluetooth device hacks.				X			X	X																					X					X
Competency 4.1 – The student will write scripts to scrape websites for information.				X			X	X																					X					X
Competency 4.2 – The student will write scripts to scrape popular social media sites for information.				X			X	X																					X					X

Competency 4.3 – The student will write scripts to spear-phish email.				X			X	X																		X				X
Competency 5.1 – The student will write malware that evades antivirus systems.				X			X	X																			X			X
Competency 5.2 – The student will write scripts to combat malware that evades antivirus systems.				X			X	X																			X			X