



El Camino College
COURSE OUTLINE OF RECORD – Official

Course Acronym:	CIS
Course Number:	121
Descriptive Title:	Cybersecurity Programming with Python
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course is an introduction to cybersecurity penetration testing using the Python programming language. The student will learn how to use Python scripting to execute effective and efficient penetration scripts focused on exposing vulnerabilities in computer systems. Topics include writing script for various types of cyber-attacks, including scanner, wireless, SQL injection, and parameter tampering.
Prerequisite:	Computer Information Systems 13 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	Computer Information Systems 119
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	Proposed
Transfer UC:	Yes
Effective Date:	Proposed
General Education: ECC	
Term:	
Other:	
CSU GE:	

Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	<p>SLO #1 Understanding Hacker Techniques</p> <p>Understanding the techniques used by hackers to crack an organization's Internet perimeter and chain exploits to gain deeper access to an organization's resources.</p> <p>SLO #2 Python Programming Language</p> <p>Demonstrate the ability to write script using the Python programming language.</p> <p>SLO #3 Penetration Tests</p> <p>Demonstrate the ability to create and execute penetration tests, report results.</p>
Course Objectives:	<ol style="list-style-type: none"> 1. Understand how to gain administrative access to systems with Python and other scripting languages using the Exploit the Remote File Inclusion. 2. Write automated scripts to gather passive information from a website and perform XSS, SQL injection, and parameter tampering attacks. 3. Develop complicated header-based attacks using script. 4. Demonstrate the understanding of the generation of Metasploit resource files and use the Metasploit Remote Procedure Call to automate exploit generation and execution.
Major Topics:	<p>I. Introduction (2 hours, lecture)</p> <p>A. Penetration Testing Methodology and Overview</p> <p>B. Types of attacks</p> <p>C. Target of attacks</p> <p>D. Vulnerability Assessments</p> <p>E. Shell Scripting</p> <p>II. Introduction to Scripting Using Python (10 hours, lecture)</p> <p>A. Installation and setup of development environment</p> <p>B. Overview of the Python programming language</p> <p>C. Variables</p> <p>D. Modules</p> <p>E. Arguments</p> <p>F. Lists</p>

G. Directories

H. Control Statements

I. File manipulation

J. Network Communications

III. Scanner Scripting (8 hours, lecture)

A. Scanning tools

B. Port Scanners

C. SSH Botnet

D. FTP Scanners

E. Service scanners

F. Metasploit

IV. Forensics Investigations (4 hours, lecture)

A. Information Gathering

B. Preparation for Penetration Testing

C. Registry

D. Metadata

V. Exploitation Scripting (8 hours, lecture)

A. Network Traffic Analysis

B. Ethernet frame architecture

C. IP Packet Architectures

D. Cross-Site Scripting

E. Database Exploitations and SQL Injections

VI. Wireless Attacks Scripting (4 hours, lecture)

A. Scapy

B. Sniffing

C. Wireless traffic interception

VII. Penetration Testing (9 hours, lab)

A. Installation and setup of development and testing environments

B. Vulnerability Assessments

C. Shell Scripting

VIII. Python Scripting (9 hours, lab)

A. Overview of the Python programming language

B. Variables

C. Modules

D. Arguments

E. Lists

F. Directories

G. Control Statements

H. File manipulation

I. Network Communications

IX. Scanner Scripting (9 hours, lab)

A. Scanning tools

B. Using Port Scanners

C. Using SSH Botnet

D. Using FTP Scanners

E. Using Service scanners

F. Using Metasploit

X. Forensics Investigations (9 hours, lab)

A. Information Gathering

B. Preparation for Penetration Testing

C. Registry Analysis

D. Metadata Analysis

XI. Exploitation Scripting (9 hours, lab)

	<p>A. Network Traffic Analysis</p> <p>B. Ethernet frame architecture</p> <p>C. IP Packet Architectures</p> <p>D. Cross-Site Scripting</p> <p>E. Database Exploitations and SQL Injections</p> <p>XII. Wireless Attacks Scripting (9 hours, lab)</p> <p>A. Using Scapy</p> <p>B. Sniffing</p> <p>C. Wireless traffic interception</p>
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Write a Python script to examine the operating system registry, to determine any programs installed or updated on a given date.
Critical Thinking Assignment 1:	Users report that data recently entered in a computer database has been altered. Examination of the network logs shows mysterious traffic from an external foreign IP address. In a one-to two-page report, describe the steps to take to determine the back-door used in the exploit.
Critical Thinking Assignment 2:	In a one-page report, list the steps you would take to determine whether a new website developed by the programming staff has SQL vulnerabilities.
Other Evaluation Methods:	Other (specify), Other Exams, Quizzes
Instructional Methods:	Demonstration, Lecture, Multimedia presentations
If other:	
Work Outside of Class:	Problem solving activity, Required reading, Study, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Textbooks:	Christopher Duffy, <u>Python: Penetration Testing for Developer</u> , PAKT, 2017.
Alternative Textbooks:	Georgia Weidman. <i>Penetration Testing: A Hands-On Introduction to Hacking</i> . 2nd ed., 2014. (Discipline Standard)

Required Supplementary Readings:	
Other Required Materials:	USB 3.0 flash drive 2 GB or larger
Requisite:	Prerequisite
Category:	sequential
Requisite course(s): List both prerequisites and corequisites in this box.	Computer Information Systems 13 with a minimum grade of C or
Requisite and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s).	Demonstrate an understanding of the development and use of information systems in business. CIS 13 - Explain the development and use of information systems in business.
Requisite Skill:	equivalent experience
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	Demonstrate an understanding of the development and use of information systems in business.
Requisite course:	Computer Information Systems 119
Requisite and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s).	Students must be able to demonstrate the knowledge necessary to create a secure computer environment, and must understand the various forms of cybercrime, how to assess a computer system for vulnerability, and various ways to secure a computer system. CIS 119 - Apply knowledge of computer hardware, software, file systems and networks in identifying and resolving computer crime and information security incidents. CIS 119 - Identify software and hardware technologies needed to defend against intrusions from adversaries, malicious actors and malware.
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Monica Chaban

Date:	04/25/2018
Original Board Approval Date:	
Last Reviewed and/or Revised by:	
Date:	
Last Board Approval Date:	12/19/2022