

CS 181.43 Course Outline as of Fall 2022**CATALOG INFORMATION**

Dept and Nbr: CS 181.43 Title: CYBER PROGRAMMING
 Full Title: Programming for Cyber Security
 Last Reviewed: 5/10/2021

Units	Course Hours per Week		Nbr of Weeks		Course Hours Total	
Maximum	3.00	Lecture Scheduled	3.00	17.5	Lecture Scheduled	52.50
Minimum	3.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	3.00		Contact Total	52.50
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 105.00

Total Student Learning Hours: 157.50

Title 5 Category: AA Degree Applicable

Grading: Grade or P/NP

Repeatability: 00 - Two Repeats if Grade was D, F, NC, or NP

Also Listed As:

Formerly:

Catalog Description:

This course offers an in-depth introduction to programming/scripting languages for system administration, web application auditing, cybersecurity and penetration testing. It provides an overview of modern scripting languages commonly used to build and extend security tools. The course will introduce students to scripting on both the Microsoft and Linux platforms and will include an overview of Powershell, Python, and other languages as the local industry dictates. Students will write programs and scripts to exercise their understanding of tools and concepts.

Prerequisites/Corequisites:

Course Completion of CS 81.21 (or CIS 50.71)

Recommended Preparation:

Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:**Schedule of Classes Information:**

Description: This course offers an in-depth introduction to programming/scripting languages for system administration, web application auditing, cybersecurity and penetration testing. It provides an overview of modern scripting languages commonly used to build and extend

security tools. The course will introduce students to scripting on both the Microsoft and Linux platforms and will include an overview of Powershell, Python, and other languages as the local industry dictates. Students will write programs and scripts to exercise their understanding of tools and concepts. (Grade or P/NP)

Prerequisites/Corequisites: Course Completion of CS 81.21 (or CIS 50.71)

Recommended: Eligibility for ENGL 100 or ESL 100

Limits on Enrollment:

Transfer Credit:

Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	Area	Effective:	Inactive:
CSU GE:	Transfer Area	Effective:	Inactive:

IGETC:	Transfer Area	Effective:	Inactive:
---------------	----------------------	------------	-----------

CSU Transfer:	Effective:	Inactive:
----------------------	------------	-----------

UC Transfer:	Effective:	Inactive:
---------------------	------------	-----------

CID:

Certificate/Major Applicable:

Both Certificate and Major Applicable

COURSE CONTENT

Student Learning Outcomes:

At the conclusion of this course, the student should be able to:

1. Write, run and execute a script based on user requirements
2. Debug and correct errors in a sample script.

Objectives:

At the conclusion of this course, the student should be able to:

1. Write simple Transmission Control Protocol/Internet Protocol (TCP/IP) networking client and server scripts and programs
2. Write scripts to simplify system administration tasks
3. Write scripts for cybersecurity and penetration testing
4. Design and implement simple programs from user requirements

Topics and Scope:

1. Introduction to Scripting Languages including PowerShell
2. Python Basics including system administration tasks
3. Setting up your Python Environment
4. TCP/IP Networks and Sockets
5. Scapy and other Tools for Cybersecurity
6. Log Analysis and Processing
7. Web Application Exploitation and penetration testing
8. Vulnerability assessment tasks and tools

- 9. Command and Control Resources, such as GitHub, Bitbucket
- 10. Trojanning Windows Systems

Assignment:

Reading assignments include:

- 1. Online research of scripting practices and methods
- 2. Approximately 50 pages weekly from the textbook

Homework problems include:

- 1. Weekly online discussion thread participation
- 2. Hands-on exercises to demonstrate proficiency with each topic
- 3. Online quizzes (5 - 12)
- 4. Assignments for scripting practices and methods

Other assignments include:

- 1. Skill demonstration examinations
- 2. Classroom scenario-based exercises

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Weekly written online discussions

Writing
5 - 10%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Homework problems, assignments for scripting practices and methods

Problem solving
15 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

Class performances of scripting practices and methods, and skill demonstration examinations

Skill Demonstrations
20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

Quizzes and skill demonstration examinations

Exams
20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Attendance and participation in scenario-based exercises

Other Category
5 - 20%

Representative Textbooks and Materials:

Bash Pocket Reference: Help for Power Users and Sys Admins. 2nd ed. Robbins, Arnold. O'Reilly. 2016 (classic)

Black hat Python: Python Programming for Hackers and Pentesters. 11th ed. Seitz, Justin. San Francisco No Starch Press. 2015 (classic)

Introduction to Scripting: National CyberWatch Center Edition. Miller & Ranum. 2017 (classic)

Learn Windows PowerShell in a Month of Lunches. 3rd ed. Jones, Don and Hicks, Jeffery. Manning Publications Co. 2016 (classic)

A Practical Guide to Linux Commands, Editors, and Shell Programming. 4th ed. Sobell, Mark G. Prentice Hall. 2017 (classic)

Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers. O'Connor, TJ. Waltham, Mass. Elsevier. 2014 (classic)