DCOM 240
Python Programming for Cybersecurity
4 Credits

Community College of Baltimore County
Common Course Outline

Description

DCOM 240 – Programming for Cybersecurity: introduces students to the fundamentals of Python programming with a focus on application in Cybersecurity, Digital Forensics and Network Technology. Designed for beginners with no prior programming experience, the course covers core programming concepts such as variables, data types, control structures, functions, file handling, and libraries. Students will gain hands-on experience using Python to solve problems relevant to the cybersecurity field including log analysis, basic network scripting and cryptography. Through a combination of lectures and lab assignments, students will learn how Python can be applied to cybersecurity field.

Pre-requisites: DCOM 142

Overall Course Objectives

Upon completion of this course, students will be able to:

1. implement development environment to run simple Python scripts;
2. apply different data types to perform basic input/output operations;
3. implement decision-making in programs using complex conditional statements;
4. implement condition-controlled and count-controlled loops in functional programs;
5. create lists, sets, dictionaries, and tuples;
6. write programs to define and call functions, use parameters and return values;
7. resolve runtime errors using exceptions with try, except, finally, and else blocks;
8. demonstrate how to open, read, write, and manage files using appropriate paths and modes;
9. apply basic object-oriented programming concepts by creating classes, objects, attributes, and methods;
10. analyze system and network information by running Python scripts;
11. develop scripts to identify operating system running services;
12. perform banner grabbing for basic operating systems (OS);
13. utilize Python libraries relevant to cybersecurity topics; and
14. automate common cybersecurity tasks with Python scripts.

Major Topics

I. Introduction to Python and Develop Environment
   a. what Python is
   b. installing Python and IDEs

c. Python syntax and commands

II. Variables, Data Types, and Basic I/O
   a. variables, strings, integers, floats, booleans
   b. user input and formatted output

III. Control Flow
   a. if/else statements, comparison operators and logical operators
   b. nesting and logical conditions
   c. condition and count-controlled loops

IV. Lists, Tuples and Basic-Object- Oriented Programming
   a. creating and modifying lists
   b. List methods (append, insert, remove, etc.)
   c. introduction to tuples and dictionaries
   d. classes and objects

V. Network Programming Basics
   a. import features
   b. gathering operating system information, sockets and running services
   c. banner grabbing
   d. analyze network traffic

VI. Automate using Python scripts
   a. Python libraries relevant to cybersecurity topics
   b. automate common cybersecurity tasks

Course Requirements

Grading will be determined by the individual faculty member, but shall include the following, at minimum:

- 10 lab activities
- 10 module quizzes
- Mid-term and final exam

Other Course Information

This course is required for Cybersecurity AAS, Cybersecurity Certificate, Digital Forensics AAS programs.

Date Revised: 11/4/2025