


QFO-AP-VA-008	رمز النموذج :	اسم النموذج : خطة المادة الدراسية	 جامعة فيلادلفيا Philadelphia University
2	رقم الإصدار: (Rev)	الجهة المصدرة: نائب الرئيس للشؤون الأكاديمية	
2021-5-4	تاريخ الإصدار:	الجهة المدققة : اللجنة العليا لضمان الجودة	
3	عدد صفحات النموذج :		

Course Title: Programming Language in Information Security	Course code: 0790220
Course Level: 2	Course prerequisite(s) and/or corequisite(s): 0721223
Lecture Time: 09:45-10:35	Credit hours: 3

Academic Staff Specifics

Name	Office Number and Location	E-mail Address
Athari Al-Natsheh		aalnatsheh@philadelphia.edu.jo

The Learning Style Used in Teaching the Course

<u>The Learning Style</u>			
Blended Learning		<input checked="" type="checkbox"/>	
Electronic Learning		<input type="checkbox"/>	
Face-to-Face Learning		<input type="checkbox"/>	
Face-to-Face	Electronic	Blended	Percentage

Course Description:

The module introduces formal techniques to support the design and analysis of Programming in Information Security, focusing on both understanding the underlying theory of networking and possible attacks and practical considerations of developed programs. Topics include socket programming, Working with N-map Scanner, Interacting with Vulnerability Scanners, Python Tools Forensics Analysis, Cryptography and Penetration testing.

Course Objectives:

The aim of this module is to learn how to Create programs for Information security. Vulnerability scanning tools, Forensic Analysis, Cryptography and Penetration testing are theoretically Analyzed and practically tested by developed programs.

Course Components

- Working with Python Scripting
- Socket Programming
- Summation Techniques
- Recurrence Relations, Tutorial
- Working with Nmap Scanner
- Interacting with Vulnerability Scanners
- Python Tools for Forensics Analysis
- Cryptography and Steganography
- Penetration Testing with Python

Textbooks:

- 1) José Manuel Ortega, Mastering Python for Networking and Security, Packt Publishing Ltd., 2020
- 2) Christopher Duffy, Learning Penetration Testing with Python, Packt Publishing Ltd. 2015.

In addition to the above, the students will be provided with handouts by the lecturer.

Teaching Methods:

Duration: 16 weeks, 48 hours in total

Lectures: 38 hours, 2 per week (including two 1-hour midterm exams)

Tutorials: 7 hours, (1 hour per 2 weeks)

Report Presentation: 3 hours

Homework: 10 assignments.

Learning Outcomes:

A- Knowledge and understanding

A1- Understanding basic ideas about programming for cybersecurity

A2- Understanding the basic concepts and protocols in Networking

A3- Understanding the behaviors of programming in Information Security

A4- Knowing and understanding a wide range of programming for Security

B- Cognitive skills (thinking and analysis).

B1- Developing efficient programs for programming in information security

B2- Reasoning about the correctness of programs and tracing them

B3- Trace and develop programs for information security

C- Communication skills (personal and academic).

C1- Ability to undertake an individual project in Security Programming.

C2- Ability to deliver a presentation for small projects.

C5- Ability to design and implement a small project using Python Programming language.

D- Practical and subject specific skills (Transferable Skills).

D3, D4, D5, D6- Display the ability to work as group and show the personal responsibilities.

Learning outcomes achievement:

Development: A1, A2, A3 and A4 are developed through lectures and home works.

B1, B2, and B3 are developed through tutorial and home works.

C1, C2, C5, D3, D4, D5, D6 are developed through assignments and essays.

Assessment : A2, A3, B1, B2, and B3 are assessed through quizzes and written exams.

C1, C2, C5, D3- D6 are assessed through projects, home works, and assignments.

Assessment Instruments

<u>Allocation of Marks</u>	
Assessment Instruments	Mark
Mid examination	30%
Final Exam (written unseen exam)	40 %
Reports, Assignments, Quizzes, Home works, Projects	30%
Total	100%

* Make-up exams will be offered for valid reasons only with consent of the Dean. Make-up exams may be different from regular exams in content and format.

Practical Submissions

The assignments that have work to be assessed will be given to the students in separate documents including the due date and appropriate reading material. Submit your home work through Teams. After the deadline “zero” will be awarded.

Course/Module Academic Calendar

Week	Basic and support material to be covered	Homework/reports and their due dates
(1)	Working With Python Scripting: Exploring Python data structures, Python Functions,	
(2)	<u>Classes, and Exceptions, Modules and packages</u>	
(3)	Managing Dependencies and developing Environments, Tutorial 1	Assignment 1
(4)	Socket Programming	
(5)	Socket Programming Tutorial 2	Assignment 2
(6)	Working With N-Map Scanner	
(7)	Interacting with Vulnerability Scanners, Tutorial 3	Assignment 3
(8)	Identifying Server Vulnerabilities in Web Applications	
(9)	Identifying Server Vulnerabilities in Web Applications,	
(10)	Identifying Server Vulnerabilities in Web Applications, Tutorial 4	Assignment 4
(11)	Python Tools for Forensics Analysis,	
(12)	<i>Python Tools for Forensics Analysis</i> , Tutorial 5	Assignment 5
(13)	Cryptography and Steganography	
(14)	Cryptography and Steganography, Tutorial 6	Assignment 6
(15)	Penetration testing in Python	
(16)	<i>Penetration testing in Python</i>	
Final Examination		

Expected workload:

On average students need to spend 2 hours of study and preparation for each 50-minute lecture/tutorial.

Attendance policy:

Absence from lectures and/or tutorials shall not exceed 15%. Students who exceed the 15% limit without a medical or emergency excuse acceptable to and approved by the Dean of the relevant college/faculty shall not be allowed to take the final examination and shall receive a mark of zero for the course. If the excuse is approved by the Dean, the student shall be considered to have withdrawn from the course.