COURSE OUTLINE

(1) GENERAL

SCHOOL	Science and Technology		
ACADEMIC UNIT	Science and Technology		
PROGRAMME OF STUDIES	MSc in Cybersecurity		
LEVEL OF STUDIES	Postgraduate		
COURSE CODE	DSC04	SEMESTER	2
COURSE TITLE	Penetration Testing		
COURSE TYPE *Elective, compulsory*	Compulsory		
INSTRUCTOR(S)	Theory: Dr. Nikolaos SERKETZIS Lab: Dr. Nikolaos SERKETZIS		

INDEPENDENT TEACHING ACTIVITIES *if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits*	WEEKLY TEACHING HOURS	CREDITS
	4,2	6
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		

TEACHING ACTIVITIES BREAKDOWN	WEEKLY HOURS
Theory	3
Lab	1
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).	

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Special background
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	English
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes
COURSE WEBSITE (URL)	https://elearn-ucips.ihu.gr/

(2) LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

On completing the course, the student will be able to:

- Familiarize with the essential terminology of the Cybersecurity domain

- Identify and being capable of performing research on the threats, vulnerabilities, exploits and risks that pertain to the cybersecurity domain
- Understand the methodology of penetration testing and apply it ensure greater levels of protection of information systems
- Develop new and improve existing technical skills

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology
Adapting to new situations
Decision-making
Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas
Project planning and management
Respect for difference and multiculturalism
Respect for the natural environment
Showing social, professional and ethical responsibility and sensitivity to gender issues
Criticism and self-criticism
Production of free, creative and inductive thinking
……
Others…
…….

- Scan information systems for identifying security vulnerabilities
- Perform open-source research to find vulnerabilities and exploits of information systems
- Select and use the appropriate tools for performing penetration tests and evaluating the relevant countermeasures for enhancing the security posture of information systems
- Decision Making
- Teamwork
- Production of free, creative, and inductive thinking

(3) SYLLABUS

The course introduces fundamental concepts and tools of Penetration Testing.

The student learns the essential background of information security and carefully moves to the methodologies used by adversaries to identify and exploit vulnerabilities of information systems. This in turns shifts him/her into proactively thinking on how to apply information security measures to protect information systems before they are being successfully taken over.

The student learns from a linear penetration testing approach, which includes the following topics

- Introduction to information security and essential terminology
- Introduction to Linux Operating Systems and Bash Scripting
- Performing passive reconnaissance
- Performing active reconnaissance
- Applying network scanning and fingerprinting
- Identifying vulnerabilities on systems and services
- Using open-source tools for researching, finding, and elaborating exploits to identified vulnerabilities
- Employing techniques for exploiting identified vulnerabilities
- Implementing post-exploitation and lateral movement

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY *Face-to-face, Distance learning, etc.*	Hybrid: Face to face and synchronous distance learning
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY *Use of ICT in teaching, laboratory education, communication with students*	**Use of ICT in Teaching** During the education process the students are provided with pre-configured Windows and Linux operating systems that have all the required tools pre-installed. The hybrid teaching method involves synchronous learning with the support of the videoconferencing tool Zoom.

Student are taught the use of the relevant tools in an innovative and constructive way through carefully crafted labs and well defined scenarios.
Students can repeat the instructions given by the lecturer during the course time. They are also given the opportunity to apply the scenarios described during the course individually, as the infrastructure is configured to be apparent on a 24/7 basis.

Use of ICT in Communication with students

- The course material (slides, scientific articles, exercises, etc.) is posted on the course page at the e-learn platform (Moodle).
- Use of Moodle Forums announcements.
- Live video meetings via Zoom/Teams.
- Contact via email.

TEACHING METHODS

The manner and methods of teaching are described in detail.
Lectures, recitation, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.

The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS

Activity	*Semester workload*
Lectures	30 hrs.
Lab	20 hrs.
Assignment	15 hrs
Exams	3 hrs.
Non-Directed Study	82 hrs.
Course total	***150 hrs.***

COURSE MATERIAL ARRANGEMENT

Theory

Introduction to information security and essential terminology	1 hr.
Introduction to Linux Operating Systems and Bash Scripting	5 hrs.
Performing passive reconnaissance	4 hrs.
Performing active reconnaissance	5 hrs.
Applying network scanning and fingerprinting	3 hrs.
Identifying vulnerabilities on systems and services	3 hrs.
Using open-source tools for researching, finding, and elaborating exploits to identified vulnerabilities	3 hrs.
Employing techniques for exploiting identified vulnerabilities	3 hrs.
Implementing post-exploitation and lateral movement	4 hrs.

Lab

Performing passive reconnaissance	3 hrs.
Performing active reconnaissance	3 hrs.
Applying network scanning and fingerprinting	3 hrs.
Identifying vulnerabilities on systems and services	3 hrs.
Using open-source tools for researching, finding, and elaborating exploits to identified vulnerabilities	3 hrs.
Employing techniques for exploiting identified vulnerabilities	
Implementing post-exploitation and lateral movement	

STUDENT PERFORMANCE EVALUATION

Language of Evaluation: English

Description of the evaluation procedure *Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other* *Specifically-defined evaluation criteria are given, and if and where they are accessible to students*	Evaluation Procedure: ● Written Exams (70%). Methods of evaluation: ○ Open-ended questions ○ Problem solving (hand-on penetration testing scenario) ○ Multiple choice questions (on lab material) ● Course Assignment (30%): ○ Information Gathering (active and/or passive reconnaissance) The evaluation procedure is announced to the students during the first lecture and is also accessible at the e-learn platform throughout the entire semester.
STUDENT OBLIGATIONS *Compulsory attendance of lectures, labs, recitations, compulsory participation in midterms, exams, compulsory delivery of homework, projects, etc.*	● Compulsory attendance of lectures ● Compulsory attendance of labs ● Compulsory participation in the exams ● Compulsory delivery of project

(5) ATTACHED BIBLIOGRAPHY

- *Suggested Bibliography*

1. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014
2. Peter Kim, The Hacker Playbook 3: Practical Guide To Penetration Testing, 2018