# FORENSICS and PENETRATION TESTING

## 1.GENERAL

| | | | |
|---|---|---|---|
| **SCHOOL** | ENGINEERING | | |
| **DEPARTMENT** | INFORMATICS AND COMPUTER ENGINEERING | | |
| **LEVEL OF STUDY** | POST-GRADUATE (7) | | |
| **COURSE UNIT CODE** | **CSCYB204** | **SEMESTER OF STUDY** | 2nd |
| **COURSE TITLE** | **Computer Forensics and Penetration Testing** | | |

| **COURSEWORK BREAKDOWN** | **TEACHING WEEKLY HOURS** | **ECTS Credits** |
|---|---|---|
| Lectures | 3 | |
| Tutorials | 2 | |
| | **5** | **8** |

| | |
|---|---|
| **COURSE UNIT TYPE** | |
| **PREREQUISITES :** | NONE |
| **LANGUAGE OF INSTRUCTION/EXAMS:** | GREEK, ENGLISH |
| **MODULE WEB PAGE (URL)** | |

## 2.LEARNING OUTCOMES

**Learning Outcomes**

PART A
Windows penetration testing
This course teaches students the underlying principles and many of the tactics, techniques, procedures and tools associated with the penetration testing or ethical hacking.
Students will learn about the entire penetration testing process including planning, OSINT, reconnaissance, scanning, Vulnerability assessment, exploitation, post exploitation, and result reporting. The course will provide the fundamental information associated with each of the methods employed by most professionals.
PART B

Windows incident handling and forensics syllabus

The Windows OS Incident handling and Forensics course covers windows memory, registry, file system and application analysis. You will build an in-house forensic capability using a variety of free, open-source, and commercial tools.

Identify and handle digital artefact/evidence to answer critical questions, including application execution, file access, data theft, external device usage, file download, anti-forensics, and detailed system usage and Implement triage, live system analysis, and alternative acquisition techniques. Compile reports and presents the findings during the digital forensics examination to the entity which was impacted by the cyberattack, or to the court for public investigation.

The objective of the course is to show students how to perform a fully digital forensic investigation of a Windows system.

**General Skills**

- Understanding the cyber threat and how cyber attackers operate.
- Understanding the tactics, techniques, procedures and tools used by penetration testers and red teams.
- Conducting a comprehensive penetration test assessment.
- Applying the cyber incident handling and response (IH&R) process.
- Conducting a comprehensive digital forensics investigation.

**3. COURSE CONTENTS**

The description contains the material to be covered during 13 lectures.

1. Introduction to Penetration Testing and Red Teaming
    a. What is a penetration test or red team assessment
    b. Penetration Test Methodology
    c. Penetration test Essentials Pre-engagement
    d. Scoping Ethical requirements and legal issues
    e. Penetration test report structure and components
    f. Building a Penetration Test lab
    g. Preparation, OSINT and anonymity infrastructure development.
2. Information Gathering
    a. Reconnaissance (DNS reconnaissance TCP, UDP, connections)
    b. OSINT (Open Source Intelligence)
    c. Scanning methodology
    d. System and network scanning, Scanning using nmap
3.vulnerability assessment
    a. Netcat
    b. Nessus
    c. OpenVas
4. Penetration test frameworks
    a. Metasploit
    b. Poshc2
    c. Covenant
    d. Mythic
5.Basics of windows security
    a. Windows internal security mechanisms
    b. Security policies
    c. Security software and devices
6. Gaining initial access
    a. Introduction to windows attacks
    b. Brute forcing
    c. Remote exploitation
    d. Client side attacks
    e. Phishing frameworks and attacks (Spear-phishing / phishing / stealing valid credentials)

7. Windows post exploitation techniques
    a. privilege escalation
    b. Lateral movement (Password Spraying, AV, EDR evasion)
    c. Powershel for penetration testers
    d. Active Directory Attacks (Kerberos Authentication, Domain enumeration, Domain attacks, Kerberoasting attack, Golden ticket, Pass the hash attack, pass the ticket, over pass the hash)
8. Incident handling process
    a. Introduction to the incident handling process
    b. Incident handling plan
9. Digital Forensics process
    a. Digital Forensics methodology
    b. Building a forensics analysis station.
    c. Building a forensics lab.
10. Windows memory forensics
    a. Memory Essentials
    b. Dumping the memory
    c. Memory analysis
11. Windows registry forensics
    a. Registry Essentials
    b. Getting the registry
    c. Registry analysis
12. Windows file system forensics
    a. Introduction to file system
    b. Gathering file system relative to case information
    c. File system analysis
    d. Windows event log analysis
13. Windows application forensics
    a. Browser Forensics
    b. Email forensics
    c. Usb forensics
    d. How to compile a comprehensive report

**4.TEACHING METHODS - ASSESSMENT**

| | |
|---|---|
| **MODE OF DELIVERY** | Face to face |
| **USE OF INFORMATION AND COMMUNICATION TECHNOLOGY** | • Use of ICT in Course Teaching<br>• Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students. |

| *Method description* | *Semester Workload* |
|---|---|
| Lectures | 39 |
| Tutorials | 26 |
| *Research work* | 50 |

| | | | |
|---|---|---|---|
| | | | |
| | Self study | 70 | |
| | ***Total course hours (25 h workload per ECTS)*** | ***200*** | |
| **ASSESSMENT METHODS** | I. A short case to analyse in class for 30 min (20%) and<br>II. Research work (80%) | | |

**5.RESOURCES**

***Essential***

- *The Hacker Playbook 3: Practical Guide To Penetration Testing by Peter Kim*
- *Incident Response with Threat Intelligence by Roberto Martínez*
- *Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8 by Harlan Carvey*

***Recommended***

- *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey*
- *Investigating Windows Systems 1st Edition, by Harlan Carvey*
- *File System Forensic Analysis 1st Edition by Brian Carrier*
- *Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition by Daniel Teixeira (Author), Abhinav Singh (Author), Monika Agarwal (Author)*
- *Penetration Tester's Open Source Toolkit 4th Edition, Kindle Edition by Jeremy Faircloth*