



UNIVERSITY OF NICOSIA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΛΕΥΚΩΣΙΑΣ

University of Nicosia, Cyprus

Course Code	Course Title	ECTS Credits
COMP-535	Ethical Hacking	10
Department	Semester	Prerequisites
Computer Science	Fall	COMP-514
Type of Course	Field	Language of Instruction
Required for <i>Cyber Security</i> concentration	Computer Science	English
Level of Course	Year of Study	Lecturer(s)
2 nd Cycle	1 st or 2 nd	Dr Harald Gjermundrød
Mode of Delivery	Work Placement	Co-requisites
face-to-face	N/A	None

Objectives of the Course:

The main objectives of the course are to:

- introduce the ethics and legal aspects of ethical hacking
- thoroughly discuss the penetration process from information gathering to the actual penetration of a system
- cover in detail the different techniques, methods, and tools used to penetrate an endpoint system
- cover in detail the different techniques, methods, and tools used to penetrate the wired and wireless infrastructure
- make students aware of common web infrastructure and applications attack vectors
- make students aware of common database vulnerabilities and attack approaches
- expose the students to potential countermeasures and how to evade these when penetrating a system.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. be aware of the ethics with respect to ethical hacking and its legal implication
2. understand the penetration process, from utilizing the human and physical element of a system, all the way through information gathering to an actual system penetration
3. be able to perform a series of zero-touch reconnaissance and information gathering process in order to facilitate an effective penetration of a system and/or site
4. apply strategies in order to compromise modern operating systems like Windows family of OSs and the Unix family of OSs
5. describe a range of approaches to compromise modern infrastructure, both wired and wireless
6. understand common web infrastructure and applications attack vectors and be able to utilize tools and skills in order to attack web infrastructures and applications
7. be apprised on common database vulnerabilities and attack approaches in order to create an effective attack against such systems
8. critically evaluate the potential countermeasures to hacking techniques in order to evade attack detection mechanisms.

Course Contents:

1. Introduction to Ethical Disclosure
 - a) Ethics of Ethical Hacking
 - b) Ethical Hacking and the Legal System
 - c) Proper and Ethical Disclosure
2. Casing the Establishment
 - a) Information Gathering and Reconnaissance
 - b) Scanning
 - c) Identifying Attack Types: Operating System, Application Level, Misconfiguration of Operating System, Services, and Applications
 - d) Gaining and Maintaining Access
 - e) Covering Tracks
3. Endpoint and Server Hacking
 - a) Hacking Windows
 - b) Hacking Unix
 - c) Cybercrime and Advanced Persistent Threats
4. Infrastructure Hacking
 - a) Remote Connectivity and VoIP Hacking
 - b) Wireless Hacking
 - c) Hacking Hardware
5. Application and Data Hacking
 - a) Web and Database Hacking
 - b) Mobile Hacking

Learning Activities and Teaching Methods:

Lectures, Lab Activities, Practical Exercises, Projects and Assignments.
--

Assessment Methods:

Projects, Lab Exercises, Mid-term Exam, Final Exam.

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
S. McClure, J. Scambray, G. Kurtz	Hacking Exposed 7: Network Security Secrets & Solutions	McGraw-Hill Osborne	2012	978-0071780285
A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey, T. Williams	Gray Hat Hacking The Ethical Hackers Handbook, 3 rd Edition	McGraw-Hill Osborne	2011	978-0071742559

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
P. Kim	The Hacker Playbook: Practical Guide To Penetration Testing	CreateSpace Independent Publishing Platform	2014	978-1494932633
B. Clark	Rtfm: Red Team Field Manual	CreateSpace Independent Publishing Platform	2014	978-1494295509
D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni	Metasploit: The Penetration Tester's Guide	NO STARCH PRESS	2011	978-1593272883
D. Stuttard, M.	The Web Application Hacker's Handbook: Finding and	John Wiley &	2011	978-

Pinto	Exploiting Security Flaws, 2 nd Edition	Sons		1118026472
-------	---	------	--	------------