

Module Title:	Penetration Testing
Module Code:	
Level:	5
Credits:	15
Pre-requisites:	None

Module Description:

IT system security is one of the key concerns of organisations today, and they need to be confident in evaluating and verifying the security of their IT systems. In this module, students will learn how to select and apply techniques such as security policy review, security audit, vulnerability analysis and penetration testing. The aim of this module is to introduce penetration techniques to test the security of an IT system under the relevant ethical and legal framework.

Indicative Content:

- System information gathering, e.g. port scanning, network discovery tool
- Perimeter testing, physical security testing
- Exploitation, e.g. metasploit Exploit Framework
- Password breaking, e.g. OPhcrack Password Cracker, Whosthere Hash Grabber
- Website exploitation, e.g. cross-site scripting, SQL injection
- Social Engineering
- Ethics and legal framework for penetration testing.

Learning and Teaching Methods:

The module will be presented through practical experiment of penetration tools and lectures that provide the opportunity for research and group work. Moodle will be used to facilitate learning.

Specific Learning Resources:

Access to PCs, on a private network, on which cyber security software and probe software can be loaded.

Bibliography

Highly Recommended

Johansen, G., Allen, L., Heriyanto, T., Ali, S. (2016) *Kali Linux 2 – Assuring Security by Penetration Test*. PACKT

McClur, S., Scambray, J. and Kurtz, G. (2012) *Hacking Exposed 7: Network Security Secrets and Solutions*. USA: McGraw-Hill

Module Specifications: Schools of Business & Management & Information Technology

Recommended

Sans Institute (2016), *CIS Critical Security Controls*. [online] Available at:

<https://www.sans.org/critical-security-controls>

Background Reading

Dhillon, G. (2006) *Principles of Information Systems Security: Text and Cases*.

Hoboken: John Wiley and sons

National Institute of Standards and Technology (NIST) Information Technology

Library <http://www.csrc.nist.gov>

The ISO 27000 Directory <http://www.27000.org>

Module Learning Outcomes

Subject Specific Learning Outcomes

On successful completion of this module you will be able to:

LO 1 | Critically evaluate and verify the security of an IT system

LO 2 | Select and apply appropriate network and system penetration techniques

LO 3 | Investigate and understand the ethical and legal framework for a penetration tester.

Assessment Title or element

Weighting (%)

Assignment: a report of the penetration test of an IT infrastructure
(late semester, 2000 words)

70%

Exam (end semester, 1hr 30min)

30%