This Version is No Longer Current

The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Penetration Testing

Reference	CM4104	Version	2
Created	May 2017	SCQF Level	SCQF 10
Approved	July 2016	SCQF Points	15
Amended	September 2017	ECTS Points	7.5

Aims of Module

To provide students with the ability to identify and exploit network security weakness within an IT infrastructure.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1 Explain and critically discuss the ethical issues relating to the performance of penetration testing.

2 Analyse and critically discuss the stages required by an ethical hacker to successfully compromise a target.

3 Critically evaluate security techniques used to protect networked systems.

4 Demonstrate a critical knowledge and understanding of the tools, methods and procedures used within the network security arena.

5 Effectively communicate the results of penetration testing.

Indicative Module Content

The ethical and legal issues relating to penetration testing Networking Protocols. Network enumeration and network mapping. Use of network sniffers Network device management and exploitation. Maintaining physical security of network devices. Utilisation of social engineering techniques Wireless technologies, security and wireless attacks Operating system security measures and weaknesses User Authentication and Cryptographic tools Standards and Best Practice Guides: ISO 27001, ISO 27005, ISO 27014.

Module Delivery

This module is taught using a structured programme of lectures, lab sessions and student centred learning.

Indicative Student Workload	Full Time	Part Time
Contact Hours	33	N/A
Non-Contact Hours	117	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4, 5
Description:	Written report.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighing of C1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in C1.
B	The student needs to achieve an B in C1.
C	The student needs to achieve an C in C1.
D	The student needs to achieve an D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CCNA 3 or equivalent.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1 McNAB,C.,2016. Network Security Assessment. O'Reilly.3rd Ed.

2 WILHELM, T., 2013. Professional Penetration Testing. Syngress.2nd Ed.

3 COLEMAN,D.D.,WESTCOTT,D.A., HARKINS,B.E. and JACKMAN, S.M. (2016) CWSP Certified Wireless Security Professional Official Study Guide: Exam PWO-204(CWNP Official Study Guides).2nd Ed. John Wiley & Sons.

4 Kim, P. (2015) The Hacker Playbook 2: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform

5 Weidman, G. (2014) Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.

6 Kolokithas, A. (2015) Hacking Wireless Networks - The ultimate hands-on guide. CreateSpace Independent Publishing Platform