This Version is No Longer Current
The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Security Testing

Reference	CMM403	Version	1
Created	April 2021	SCQF Level	SCQF 11
Approved	July 2021	SCQF Points	30
Amended		ECTS Points	15

Aims of Module

To enable students to apply strategies for identifying security vulnerabilities in applications, systems and networks.

Learning Outcomes for Module

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

1	Critically analyse the vulnerabilities, and their potential for exploitation, to computer applications, systems and networks.
2	Apply a range of specialised penetration testing methods and tools to exploit the vulnerabilities.
3	Develop appropriate remediation of vulnerabilities and recommendations.
4	Discuss the ethical issues pertaining to performing security testing.

Indicative Module Content

The ethical, legal and organisation's policies of security testing. Developing testing plans. OSINT, Footprinting, Scanning, Enumeration, Vulnerability identification, assessment and exploitation. Software Security vulnerabilities (e.g. CVE, CWE), Software Security testing (e.g. static/dynamic code analysis), Secure Software Lifecycle, Security by design. Penetration testing of web applications, operating systems and networks. Use of security testing frameworks (e.g., OWASP Top 10 for web applications). Use of security testing platforms and tools (e.g., nmap, Metasploit, OpenVAS). Reporting results. Recommending and implementing appropriate remediation and security hardening enhancements to protect assets.

Module Ref:	CMM403 v1

Module Delivery

The module is delivered via work-based learning along with structured online learning materials/activities and directed study, facilitated by regular online tutor support. Workplace Mentor support and work-based learning activities will allow students to contextualise this learning to their own workplace. Face-to-face engagement occurs through annual induction sessions, employer work-site visits, and modular on-campus workshops. Study Groups will be formed to encourage students to work collaboratively on set learning activities and share practice from their workplaces. Formative feedback will be provided to make sure teams are engaging positively and performing effectively.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	30	N/A
Placement/Work-Based Learning Experience [Notional] Hours	240	N/A
TOTAL	300	N/A
Actual Placement hours for professional, statutory or regulatory body	240	

ASSESSMENT PLAN

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

Component 1

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	1, 2
Description:	Report on the methods of a penetration testing exercise for a given scenario.				

Component 2

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	3, 4
Description:	Report on findings and recommendations.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 and 50% weighting of C2 components. An overall minimum grade D is required to pass the module.

		Coursework:						
		A	**B**	**C**	**D**	**E**	**F**	**NS**
Coursework:	**A**	A	A	B	B	C	E	
	B	A	B	B	C	C	E	
	C	B	B	C	C	D	E	
	D	B	C	C	D	D	E	
	E	C	C	D	D	E	E	
	F	E	E	E	E	E	F	
	NS	Non-submission of work by published deadline or non-attendance for examination						

Module Ref:	CMM403 v1

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	McNAB, C., 2016. Network Security Assessment. O'Reilly.3rd Ed.
2	SAGAR, R., 2019. Quick Start Guide to Penetration Testing With NMAP, OpenVAS and Metasploit. Apress.
3	Du, W., 2019. Computer Security: A hands-on Approach. Wenliang Du. 2nd Ed.
4	VELU, V. K., BEGGS, R., 2019. Mastering Kali Linux for advanced penetration testing: secure your network with Kali Linux 2019.1 - the ultimate white hat hackers' toolkit. Packt Publishing.
5	KHAN, F., 2019. Hands-on penetration testing with python: enhance your ethical hacking skills to build automated and intelligent systems. Packt Publishing.
6	YAWORSKI, P., 2019. Real-world bug hunting: a field guide to web hacking. No Starch Press.