Title:	Security Penetration Testing APPROVED
Long Title:	Security Penetration Testing

Module Code:	COMP8028	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Advanced
Field of Study:	Computer Science
Valid From:	Semester 1 - 2017/18 (September 2017)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	Sean McSweeney

Module Description:	Penetration Testing is the process of attacking a computer system to identify and verify security weaknesses. Penetration is essential in determining the real-world feasibility of a given set of attack vectors and testing the ability of network defenders to react and respond to a hostile presence. Penetration Testing is a vital component in maintaining a strong security posture in enterprise environments. This module covers the terminology and techniques used in network penetration testing. The learner will develop both theoretical knowledge of the activities of a penetration tester and the trade-craft necessary to perform network penetration testing.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Assess the steps involved in the planning, scoping and reconnaissance phase of a network penetration test.
LO2	Appraise the tools and techniques used for computer network mapping and vulnerability assessment.
LO3	Evaluate exploitation techniques, frameworks and tools.
LO4	Compare post exploitation techniques and tools.
LO5	Compare password hash generation, storage and use for authentication across a network

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.*
No requirements listed

Module Content & Assessment

Indicative Content
Reconnaissance Techniques Obtaining basic DNS information (Whois, nslookup), performing zone transfers (dig), DNS interrogation. Google hacking, reconnaissance tools (Spiderfoot) and open source reconnaissance frameworks (Recon-ng).
Scanning Techniques Port scanning, network mapping and OS fingerprinting (nmap). Vulnerability scanning (OpenVAS).
Exploitation & Backdoors Exploitation frameworks (Metasploit), Backdoor kits (BO2K), Exploit crafting.
Post Exploitation Obtaining credentials, pivoting (meterpreter), relays (netcat), shell vs. terminal access, privilege escalation
Passwords Password Hash Representation methods, salt, password cracking (Cain), rainbow tables (John), passwords crossing a network (SMBus).

Assessment Breakdown	%
Course Work	50.00%
End of Module Formal Examination	50.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	The learner's understanding of some of the tools and techniques used by hackers to perform reconnaissance, network mapping, vulnerability assessment, exploitation, pivoting, maintaining access and cracking credentials to resources in a network will be assessed through a project consisting of a penetration test.	1,2,3,4,5	50.0	Week 10

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	End of Semester Formal Examination.	1,2,3,4,5	50.0	End-of-Semester

Reassessment Requirement
Repeat examination *Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.*

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & directed learning.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & directed learning.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

- **Daniel W. Dieterle 2016, *Basic Security Testing with Kali Linux 2*, McGraw-Hill [ISBN: 9781530506569]**

Supplementary Book Resources

- **Peter Kim 2015, *The Hacker Playbook 2: Practical Guide To Penetration Testing* [ISBN: 9781512214567]**
- **Ben Clark 2014, *Rtfm: Red Team Field Manual*, 1st Ed. [ISBN: 9781494295509]**
- **Peter Kim 2014, *The Hacker Playbook: Practical Guide To Penetration Testing* [ISBN: 9781494932633]**

Supplementary Article/Paper Resources

- **Sarraute, C., Buffet, O. and Hoffmann, J. 2013, *POMDPs make better hackers: Accounting for uncertainty in penetration testing*., 26th Conference on Artificial Intelligence, Toronto, Canada**
- **Jajodia, S. Noel, S. and O'Berry, B. 2005, *Topological analysis of network attack vulnerability*, Managing Cyber Threats, Springer**

Other Resources

- **Website: Offensive Security*Metasploit Unleashed***
  https://www.offensive-security.com/metas ploit-unleashed/
- **Website: *Kali Linux***
  https://www.kali.org/
- **Website: *SecTools***
  http://sectools.org/

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KDNET_8	Bachelor of Science (Honours) in Computer Systems	8	Elective
CR_KITMN_8	Bachelor of Science (Honours) in IT Management	8	Mandatory