H8PENT: Penetration Testing

Module Code:	H8PENT
Long Title	Penetration Testing APPROVED
Title	Penetration Testing
Module Level:	LEVEL 8
EQF Level:	6
EHEA Level:	First Cycle
Credits:	10
Module Coordinator:	
Module Author:	Alex Courtney
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	MSc and/or PhD degree in computer science or cognate discipline. May have industry experience also.

Learning Outcomes

On successful completion of this module the learner will be able to:

#	Learning Outcome Description
LO1	Examine and assess network and application security characteristics and establish the scope and objectives of security penetration testing of digital systems.
LO2	Design, develop, and implement a security test for applications and network infrastructure while considering the ethical implications.
LO3	Apply appropriate tools and techniques during a penetration test so that the full scope and objectives of the security test are achieved.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	Learners should have attained the knowledge, skills and competence gained from stage 3 of the BSc (Hons) in Computing.

H8PENT: Penetration Testing

Module Content & Assessment

Indicative Content
Introduction and Background Hacking history, motivations and impact. Review of attack types (e.g., malware, vulnerability exploits, social engineering). Overview of security testing and incident response. How to become an ethical hacker (e.g., certifications). Ethical aspects of penetration testing
Penetration Testing Methodologies Layered attack vectors (e.g., networks, systems, applications, user). Vulnerability assessment vs. penetration testing. Testing approaches (e.g., Whitebox, greybox, blackbox). Internal and external testing. Offensive and defensive testing (e.g., red vs. blue vs. purple teams). Overview of penetration testing methodologies (e.g., PTES, OSSTMM, NIST 800-115)
Network Security Review of networking concepts and fundamentals. Common protocols and their function. Overview of attacks and mitigation solutions for different layers of the TCP/IP protocol suite. Principle of least privilege, access control, and operating systems security. Secure Network Architecture. Securing network components and communications
Network Penetration Testing Open source intelligence (OSINT) - gathering information from public sources. Fingerprinting and footprinting techniques for discovering hosts and services running on a network. Identifying protection mechanisms (e.g., firewalls). Threat modelling. Vulnerability analysis - identifying flaws in systems and applications and reasons why they are vulnerable. Potentially exploiting the vulnerabilities to gain unauthorised access to parts of the network. Post-exploitation (e.g., infrastructure analysis, pillaging, data exfiltration, pivoting to gain access to other parts of the network, persistence)
Wireless Security and Attacks Common wireless protocols and vulnerabilities in these protocols (e.g., IEEE 802.11). Wi-Fi attacks
Web Penetration Testing Industry standard vulnerability lists such as the OWASP Top 10 and the CWE/SANS Top 25. Web application vulnerability scanners and tools. Penetration testing of web application flaws (e.g., Injection, Authentication and Authorization bypass, Cross Site Scripting, Cross Site Request Forgery, Security Misconfiguration)
Mobile Penetration Testing Common security vulnerabilities in mobile devices, and impact on different Mobile OS. Insecure data storage in the device and in transit. Client-side attacks, application permissions, untrusted inputs. Binary protections and poor authorization and authentication

Assessment Breakdown	%
Coursework	50.00%
End of Module Assessment	50.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities.

Assessment Type:	Continuous Assessment	**% of total:**	50
Assessment Date:	n/a	**Outcome addressed:**	2,3
Non-Marked:	No		

Assessment Description:
The continuous assessment will focus on the practical aspects of penetration testing. Learners will have to apply appropriate tools and technique to conduct penetration testing activities on one or more operating systems, networks or applications. Learners will have to document their findings in a report they will submit for assessment.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	50
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2
Non-Marked:	No		

Assessment Description:
Learners are required to complete a formal end-of-semester examination.

No Workplace Assessment

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.

Reassessment Description
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 reassessment strategy for this module will consist of a written examination that will assess all learning outcomes. Learning EnvironmentLearning will take place in a classroom/lab environment with access IT resources. Learners will have access to library resources, both physical and electronic and to faculty outside of the classroom where required. Module materials will be placed on Moodle, the College's virtual learning environment

H8PENT: Penetration Testing

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom & Demonstrations (hours)	24	Every Week	24.00
Tutorial	Other hours (Practical/Tutorial)	24	Every Week	24.00
Independent Learning	Independent learning (hours)	202	Every Week	202.00
			Total Weekly Contact Hours	48.00

Module Resources

Recommended Book Resources

Gus Khawaja. Practical Web Penetration Testing, [ISBN: 978-1788624039].

OWASP Testing Guide v4, https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents.

Shamal Faily, John McAlaney, Claudia Iacob.. (2015), , Ethical Dilemmas and Dimensions in Penetration Testing, International Symposium on Human Aspects of Information Security & Assurance (HAISA.

Justin Pierce, Ashley Jones, Matthew Warren.. (2006), , Penetration Testing Professional Ethics: a conceptual model and taxonomy, Australasian Journal of Information Systems, 13(2), p, org/10, 8, https://doi.

Supplementary Book Resources

Jim O'Gorman,Devon Kearns,Mati Aharoni. (2011), Metasploit, No Starch Press, p.328, [ISBN: 9781593272883].

Dominic Chell,Tyrone Erasmus,Shaun Colley,Ollie Whitehouse. (2015), The Mobile Application Hacker's Handbook, John Wiley & Sons, p.816, [ISBN: 978-1118958506].

Dafydd Stuttard,Marcus Pinto. (2011), The Web Application Hacker's Handbook, John Wiley & Sons, p.912, [ISBN: 978-1118026472].

Peter Kim. (2018), The Hacker Playbook 3, Hacker Playbook, p.290, [ISBN: 978-1980901754].

Article/Paper List.

Type.

Item.

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note:	