H8PENTST: Network and Web Penetration Testing

Module Code:	H8PENTST
Long Title	Network and Web Penetration Testing APPROVED
Title	Network and Web Penetration Testing
Module Level:	LEVEL 8
EQF Level:	6
EHEA Level:	First Cycle
Credits:	5
Module Coordinator:	Arghir Moldovan
Module Author:	Arghir Moldovan
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 web 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	See Section 4.2 Entry Procedures and Criteria for the programme.

H8PENTST: Network and Web 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)
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)

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 (0200)	**% 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
The reassessment strategy for this module will consist of a written examination that will assess all learning outcomes.

H8PENTST: Network and Web Penetration Testing

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Per Semester	2.00
Tutorial	No Description	24	Per Semester	2.00
Independent Learning	No Description	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Per Semester	2.00
Tutorial	No Description	24	Per Semester	2.00
Independent Learning	No Description	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

Georgia Weidman. (2014), Penetration Testing: A Hands-On Introduction to Hacking, 1st Edition. No Starch Press, p.528, [ISBN: 978-1593275648].

Gus Khawaja. (2018), Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more, Packt Publishing, p.294, [ISBN: 978-1788624039].

Supplementary Book Resources

Peter Kim. (2018), The Hacker Playbook 3: Practical Guide to Penetration Testing, Secure Planet, p.290, [ISBN: 978-1980901754].

David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni. (2011), Metasploit: The Penetration Tester's Guide, 1st Edition. No Starch Press, p.328, [ISBN: 9781593272883].

Dafydd Stuttard, Marcus Pinto. (2011), The Web Application Hacker's Handbook, 2nd Edition. John Wiley & Sons, p.878, [ISBN: 978-1118026472].

Recommended Article/Paper Resources

OWASP Testing Guide v4,
https://www.owasp.org/index.php/OWASP_Te sting_Guide_v4_Table_of_Contents

Justin Pierce, Ashley Jones, Matthew Warren. (2006), Penetration Testing Professional Ethics: a conceptual model and taxonomy, Australasian Journal of Information Systems, 13(2), p.8,
https://doi.org/10.3127/ajis.v13i2.52

Shamal Faily, John McAlaney, Claudia Iacob. (2015), Ethical Dilemmas and Dimensions in Penetration Testing, International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), p.10,
https://cybersecurity.bournemouth.ac.uk/ wp-content/papercite-data/pdf/fami15.pdf

Other Resources

[Website], CISSP – Certified Information Systems Security Professional,
https://www.isc2.org/Certifications/CISS P

[Website], CWE/SANS Top 25 Most Dangerous Software Errors,
https://cwe.mitre.org/top25/

[Website], OWASP Top 10,
https://www.owasp.org/index.php/Top_10_2 013-Table_of_Contents

[Website], Kali – Linux Penetration Testing Distribution,
https://www.kali.org/

[Website], Metasploit Unleashed – Free Ethical Hacking Course,
https://www.offensive-security.com/metas ploit-unleashed/

[Website], Burp Suite,
https://portswigger.net/burp/

[Website], OWASP Zed Attack Proxy (ZAP),
https://www.owasp.org/index.php/OWASP_Ze d_Attack_Proxy_Project

Discussion Note:	