H9NSPT: Network Security and Penetration Testing

Module Code:	H9NSPT
Long Title	Network Security and Penetration Testing APPROVED
Title	Network Security and Penetration Testing
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	10
Module Coordinator:	Vanessa Ayala-Rivera
Module Author:	Margarete Silva
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Critically assess network security characteristics and determine the scope of a penetration test of a network system.
LO2	Design, develop, and implement a security test on a network infrastructure.
LO3	Research and critically analyse network security vulnerabilities, as well as mitigation solutions.
LO4	Justify the choice of tools and techniques that are employed for penetration tests and evaluate the results of these tests.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9NSPT: Network Security and Penetration Testing

Module Content & Assessment

Indicative Content
Introduction and Background Module overview Hacking history, motivation, and impact Why emphasis is on security testing and response to vulnerabilities is essential, and the impact that follows a breach Overview of attack types and mitigations What is penetration testing Related terminologies (e.g., capture the flags, bug bounties) How to become an ethical hacker (e.g., certifications) Ethical aspects of penetration testing
Network Principles and Fundamentals Review of core networking concepts OSI model and TCP/IP protocol suite Transport protocols and their function Common application layer protocols and network services Security protocols
Network Security Overview of attacks and mitigation solutions for different layers of the TCP/IP suite Types of networks Secure network architecture and concepts (e.g., principle of least privilege, DMZ, network segregation, zero trust, etc.) Overview and types of network security systems (e.g., firewall, IDS/IPS, XDR, WAF, honeypot, etc.)
Penetration Testing Methodologies and Information Gathering Testing approaches (e.g., whitebox, greybox, blackbox) Offensive and defensive testing (e.g., red vs. blue vs. purple teams) Overview of penetration testing methodologies (e.g., PTES, OSSTMM, NIST 800-115) Reconnaissance / passive information gathering / OSINT Active network information gathering (e.g., port scanning, service enumeration, automatic vulnerability scanning and analysis, etc.)
Authentication Attacks and Human Trust Exploits Hashing vs. encryption Authentication systems, and methods to increase their security Human factors and issues Password managers and their vulnerabilities Password attacks Social Engineering, Human factors and issues
Network Exploits Exploit types Exploitation prerequisites and challenges Finding exploits Overview of network exploitation frameworks (e.g., Metasploit)
Post-exploitation Information gathering and exfiltration Persistence mechanisms Privilege escalation Dealing with logging Evasion techniques Pivoting / lateral movement
Web Vulnerabilities and Testing Overview of the OWASP Top 10 Testing for web application vulnerabilities (e.g., injection, cross site scripting, authentication failures, etc.) Overview of web application vulnerability scanners and tools
DDoS Overview of Distributed Denial of Service (DDoS) attacks and motives Types of attacks Mitigation solutions Impact of Internet of Things (IoT) growth
Wireless Networks Overview Overview of wireless networking concepts (e.g., RF waves, spectrum, modulation, multiplexing, etc.) Wireless network types Wireless technologies and standards (e.g., WiFi, Bluetooth, LTE, 5G, etc.)
Wireless Security WiFi security and authentication standards (e.g., WEP, WPA1/2/3) WiFi vulnerabilities and attacks Overview of vulnerabilities and attacks for other wireless technologies and devices (e.g., routers, Bluetooth, RFID, NFC, IoT, etc.)
Revision Revision and catch-up

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	CA 1	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	2,4
Non-Marked:	No		

Assessment Description:
For this CA learners will work in groups, to carry out penetration testing activities on several recent vulnerable systems that are available through public online learning platforms. Each group will have to write and submit a report documenting their work, as well as present their work to the class.

Assessment Type:	CA 2	**% of total:**	60
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
The terminal assessment will be individual and assess all the learning outcomes. For this assessment learners will have to research and define a complex and realistic network setup, including recent devices and software. Moreover, they will research recent attack vectors that hackers could use to gain access to the network, as well as mitigation solutions to protect against such attacks. The final submission will be a written report documenting the research carried out.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Reassessment Description
The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.

H9NSPT: Network Security and 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 and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	4.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	24	Per Semester	2.00
Independent Learning Time	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom lecture	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Tutorial	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	20.83

Module Resources

Recommended Book Resources

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

William Stallings. (2016), Network Security Essentials: Applications and Standards, 6th Edition. Pearson, [ISBN: 978-0134527338].

Allen Harper, Ryan Linn, Stephen Sims, Michael Baucom, Huascar Tejeda, Daniel Fernandez, Moses Frost. (2022), Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition, 6th Edition. McGraw-Hill Education, p.752, [ISBN: 978-1264268948].

Supplementary Book Resources

Glen D. Singh. (2022), The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire, 2nd Edition. Packt Publishing, p.742, [ISBN: 978-1801818933].

Wil Allsopp. (2017), Advanced Penetration Testing: Hacking the World's Most Secure Networks., Wiley, p.288, [ISBN: 978-1119367680].

This module does not have any article/paper resources

Other Resources

[Other], J. Pierce, A. Jones, M. Warren. (2006), Penetration Testing Professional Ethics: a conceptual model and taxonomy, Australasian Journal of Information Systems, 13(2),
https://doi.org/10.3127/ajis.v13i2.52

[Other], S. Faily, J. McAlaney, C. 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

Discussion Note:	