Manchester Metropolitan University

Unit Specification (Collaborative/Postgraduate/Flexible Framework Use Only)

Unit Details & Outline

Unit Title	Advanced Network Security		
Unit Code	6G7Z1010		
Unit Abbreviation	Adv Net Sec		
Level of Study	7		
Credit Value	30	**ECTS Value**	15
Home Department	Division of Computer Science and Information Systems School of Computing, Mathematics and Digital Technology		
Home Faculty	Science and Engineering		
Unit Co-ordinator	Thomas Martin, Robert Hegarty		
Key Words	Network security, Intrusion detection, wireless network security, Cloud scurity, Ethical hacking		

Unit Description

Brief Summary	The aim of this unit is to provide student with the necessary skills to design and implement advanced security machanism in a network environment. It will look in depth in relation to wired and wireless network secrity and the best practices in the field.
Indicative Content	The unit starts with a general overview of the topic of Network Security, including motivation, application, and some general concepts. [16%] The unit covers Ethical Hacking: how it can be used as part of an organisation's regular security maintenance, precautions that need to be followed, and general stages of operation. [17%] The construction of network protocols is explored, including the use of symmetric and asymmetric encrypt, directional and mutual authentication, and the inclusion of trusted third-parties. Examples of exchanges are analysed, the security they try to achieve and the ways in which they can be subverted. [17%]

	Various approaches and techniquest for mitigations of threats are discussed and compared, including the use of vulnerability assessment tools. [17%] Specific attacks at various layers of the network stack are explored. Important network security protocols are examined (IPSec, SSL/TLS), including their benefits and short-comings. [17%] Finally, various topics that touch on network security are surveyed: Wireless networks, Mobile networks, Cloud, BYOD, Web security, DNS Security. [16%]

Learning Outcomes

Unit Learning Outcomes	On successful completion of this unit students will be able to: 1. Crictically analyse and evaluate the current and emerging trends in network security and its deployment in an organisation; 2. Explain and critically analyse a variety of security attacks and propose appropriate security mechanisms to detect/prevent such attacks; 3. Identify and conduct the high-level design of secure network applications; 4. Use appropriate network development tools in the deployment of secure computer networks.

Assessment

Summative Assessment

Element	Type	Weighting	Learning outcomes assessed
1	Coursework	50%	1,2
2	Examination	50%	3,4

Employability and Sustainability Outcomes

Outcomes	Element of Assessment
Apply skills of critical analysis to real world situations within a defined range of contexts.	1
Demonstrate a high degree of professionalism.	
Express ideas effectively and communicate information appropriately and accurately using a range of media including ICT.	1
Develop working relationships using teamwork and leadership skills, recognising and respecting different perspectives.	1

	Manage their professional development reflecting on progress and taking appropriate action.	
	Find, evaluate, synthesise and use information from a variety of sources.	1
	Articulate an awareness of the social and community contexts within their disciplinary field.	
	Use systems and scenario thinking.	2
	Engage with stakeholder/interdisciplinary perspectives.	
Description of each element of Assessment	**Summative** Element 1: Students will deploy a virtualised computer network and demonstrate the use of ethical hacking techniques to appraise its security. • Report (85%) to be around 2,000 words assessing LO1 and LO2 • Students will also deliver a presentation (15%) on their investigation Element 2: This assessment will be a three hour examination. The examination will assess a student's knowledge of key elements within the curriculum. Students will be required to provide correct and comprehensive answers to questions and demonstrate correct and appropriate application of techniques. As a general guide, students awarded marks within the Distinction band will perform strongly against virtually all appropriate criteria. Students awarded a mark within the Merit band will perform well against most criteria. Students awarded a pass mark will perform adequately against most criteria. **Formative** Students recieve formative feedback during supported weekly laboratory sessions.	
Mandatory Learning & Teaching Requirements	N/A	
Minimum Pass Mark	N/A	

Learning Activities

Breakdown of Student Learning Activity	**Type of Activity**	**%**
	Summative Assessment	25%
	Directed Study	25%
	Student-centred Learning	50%

Learning Resources

Books recommended for purchase by students	None
Essential Reading/ Resources	Weidman G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press, ISBN 978-1593275648
Further Reading/ Resources	Kim P. (2018) *The Hacker Playbook 3: Practical Guide to Penetration Testing,* SecurePlanet, ISBN: 978-1980901754 Stallings W. (2016) *Cryptography and Network Security: Principles and Practice*, Pearson, 7th Ed. ISBN 13 978-9332585225 Simpson M. T. and Antill N. (2016) *Hands-On Ethical Hacking and Network Defense*, Delmar Cengage Learning, ISBN 13 978-1285454610 Bejtlich R. (2013) *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, ISBN 13 978-1593275099 O'Connor T. J. (2012) *Violent Python: A Cookbook for Hackers*, *Forensic Analysts,* *Penetration Testers and Security Engineers*, Syngress, ISBN 13 978-1597499576 Mcclure S., Scambray J., Kurtz G. (2012) *Hacking Exposed 7: Network Security Secrets & Solutions*, McGrawSHill Osborne, 7th Ed. ISBN 13 978-0071780285 Vyacheslav F. (2013) *Instant Penetration Testing – Setting Up a Test Lab How-to*, Packt Publishing, ISBN 978-1285454610 Engebretson P. and Kennedy D. (2013) *The Basics of Hacking and Penetration Testing*, Syngress ISBN: 9780124116412
Specialist ICTS Resources	Hardware and software requirements decided annually and communicated to specialist technical support.
Additional Requirements	None

Administration

JACS Code	I100
HESA Academic Cost Centre	121 IT, Systems Sciences and Computer Software Engineering (C1)
Date of	19 December 2013

Approval	
Date of Most Recent Consideration	19 December 2013
Unit External Examiner	Prof. Reinhold Behringer
Unit Assessment Board	Science and Engineering