Prifysgol Glyndŵr Wrecsam | Wrexham Glyndŵr University

MODULE SPECIFICATION PROFORMA

Module Code:	COM642

Module Title:	Ethical Hacking

Level:	6	**Credit Value:**	20

Cost Centre(s):	GAPC	JACS3 **code**:	I190

Faculty:	Arts, Science and Technology	**Module Leader:**	Dr. Paul Comerford

Scheduled learning and teaching hours	24 hrs
Guided independent study	176 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
BSc (Hons) Cyber Security	✓	□
BSc (Hons) Computer Networks and Security	✓	□
BSc (Hons) Applied Cyber Security	✓	□

Pre-requisites
None

Office use only

Initial approval: 30/08/2018 Version no:2

With effect from: 01/09/2018

Date and details of revision: Jan 22: addition of BSc Applied Cyber Security Version no:

Module Aims

The module aims to give students a solid and professional level of competence in the field of ethical hacking, which is predominantly led by the coverage of tools, techniques and systems that allow penetration testing to be carried out on computer systems and networks. Much of the module material follows the footsteps of a would-be intruder and thus includes coverage of the communication and social side of computer attacks as well as the technological. Having been led to understand how systems, software and devices can be vulnerable to unwanted penetration, students will then investigate countermeasures and organisational strategies to mitigate these risks. The module leans towards practical skills and content, but is strongly underpinned by theory and current research.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Differentiate between a range of threats and techniques used in attacks on computer systems	KS1	KS4
		KS5	KS 6
2	Investigate ethical and legal issues surrounding cyber security	KS 1	KS 3
		KS 4	KS 5
		KS 6	KS 9
3	Evaluate computer systems and networks to identify weaknesses and vulnerabilities in an ethically sound manner	KS 1	KS 3
		KS 4	KS 5
		KS 6	KS 10
4	Synthesise a series of technological interventions to address computer security problems	KS 2	KS 3
		KS 4	KS 9
		KS10	

Transferable skills and other attributes

- Personal motivation, organisation and time management
- Ability to collaborate and plan
- Written and verbal communication skills
- Research and analytical skills

Derogations

None

Assessment:

Indicative Assessment Tasks:

Reflecting the nature of the learning outcomes, assessment is divided between evaluation of students' acquisition of theory, current research, and practical abilities. In the first component, students will be required to produce a report based upon recent or emerging types of cyber attack. They should describe these attacks and their solutions at a deep, technical level and contextualise them from data, privacy, ethical, legal, and social perspectives. The second assignment will require students to demonstrate their practical abilities in the domain of penetration testing, information gathering, and problem-solving abilities. For example, students in this assignment may role play attacker and system administration in a type of 'war game' before swapping roles.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1, 2	Report	40		2,000
2	3, 4	Practical	60		3 hours

Learning and Teaching Strategies:

This module has an emphasis in the practical issues related to Ethical Hacking and will be delivered using a combination of formal lecturers, tutorials, practical demonstrations and lab sessions. The split between theory and practical teaching and learning is approximately 40% and 60% respectively. The formal delivery will be supplemented by reading materials, such as academic papers and industry technology reports, which will be made available via the University's VLE.

Syllabus outline:

- Information gathering and social engineering
- Ports and protocols
- Data privacy
- Attacks from within an organisation
- Penetration testing and fuzzing
- Exploiting vulnerabilities
- Windows and Linux local system exploits and attacks
- Software vulnerabilities
- Ethics of penetration testing
- Wireless network attacks
- Smartphone and mobile device exploits
- Cyber crime and the law
- Logging and responding to incidents
- Disaster and recovery strategies

Indicative Bibliography:

Essential reading

McClure, S., Scambray, J., and Kurtz, G. (2012). *Hacking Exposed: Network Security Secrets and Solutions*. 7th ed. New York: McGraw-Hill/Osborne.

Shema, M. and Johnson, B.C. (2014), *Anti-Hacker Tool Kit*. 4th ed. New York: McGraw-Hill/Osborne.

Wrightson, T. (2014). *Advanced Persistent Threat Hacking: The Art and Science of Hacking any Organization.* New York: McGraw-Hill/Osborne.

Weidman, G., (2014). *Penetration Testing: A Hands-on Introduction to Hacking*. No Starch Press.

Other indicative reading

Conheady, S. (2014). *Social Engineering in IT Security: Tools, Tactics and Techniques*. New York: McGraw/Osborne.

IEEE Security & Privacy Magazine, IEEE
Computers and Security (journal), Elsevier Publishing
Journal of Cybersecurity, Oxford University Press
Journal of Cyber Security Technology, Taylor and Francis