UNIVERSITY of BRADFORD

Module Descriptor

Module Details	
Module Title	Ethical Hacking
Module Code	COS7029-B
Academic Year	2024/5
Credits	20
School	School of Computer Science, AI and Electronics
FHEQ Level	FHEQ Level 7

Contact Hours	
Type	Hours
Lectures	12
Laboratories	36
Directed Study	152
Lectures	12

Availability	
Occurrence	Location / Period
BDA	University of Bradford / Semester 2

Module Aims

Ethical hacking, a key area of cyber defence, protects businesses from the wide-ranging impact of cyber-attacks. It is, essentially, a security audit, where the company hires an ethical (white hat) hacker to identify and draw up a report on all possible vulnerabilities. This report provides details on all potential pathways by which hackers could gain access to an organisation?s information systems.

This module aims to instil in students an in-depth understanding of underlying principles and techniques associated with ethical hacking and penetration testing to identify security vulnerabilities and strengthen a target system's defences against cyber threats. The module will give you an understanding of developing appropriate procedures, solutions and mitigation measures to defend and minimise risks of malicious hacking attacks targeting computing systems.

Outline Syllabus

The outline syllabus indicates the topics that you will study. This information may change, so please keep a record of any module announcements regarding changes from your Module Tutor via CANVAS. This module will cover these key topics:

Introduction to ethical hacking: Basics of ethical hacking, information security controls, relevant laws (PCI, DSS, HIPPA, etc.), and standard procedures.

Stages of ethical hacking: Footprinting and reconnaissance, Network scanning, Enumeration, and System hacking.

Malware: Malicious activities, malware analysis and detection techniques
Vulnerability analysis: Types, detection, pen tests, and prevention of vulnerabilities
Sniffing: Types, detection, ethical issues, pen tests, and prevention of sniffing
Social engineering: Types, insider threats, attacks, and preventive measures
SQL injection: Types, IDS evasion techniques, ethical issues, pen tests, and countermeasures
Session hijacking: Types, ethical issues, pen tests, and preventive measures
Hacking web servers: Types of web server attacks, ethical issues, pen tests, and preventive measures

Learning Outcomes

Outcome Number	Description
01	Explain constitutive concepts and methods of the penetration testing process, including planning, reconnaissance, scanning, exploitation, and post-exploitation.
02	Demonstrate appropriate use of basic and advanced hacking tools to perform penetration testing.
03	Develop analytical skills in relation to identifying weaknesses and vulnerabilities of the systems.
04	Describe and critically assess the mitigation techniques for offensive penetration techniques.
05	Describe the ethical and legal issues related to penetration testing.
06	Apply research and problem-solving skills by logically and persuasively supporting their findings or points of view.

Learning, Teaching and Assessment Strategy

Students will develop the knowledge, understanding, and skills necessary to meet the module's learning outcomes through lectures, lab sessions and independent study. Formal lectures will outline the theoretical principles of ethical hacking and penetration testing. Students will participate in practical lab exercises to learn how to effectively scan, test, and hack to secure systems in accordance with ethical and legal considerations. This lab-intensive module facilitates knowledge acquisition and practical experience with current security systems (LO1- LO6).

Utilising current research and industry trends in cyber security, the students will participate in lectures, labs, and independent study to explore the latest hacking tools, techniques, and methodologies used by hackers and information security professionals to hack an organisation lawfully.

To support accessibility, clarity and comprehension, all teaching material is provided on CANVAS wherever possible in advance of the teaching sessions. Throughout the programme, students are provided opportunities to demonstrate their skills and express their ideas, choosing from various ethical hacking tools and techniques.

To prepare the students for employment in the real world, assessments are designed to measure industry-needed skills, such as conducting vulnerability analysis on target systems, performing penetration testing using the latest hacking tools, and documenting the penetration test reports. Throughout the module, students will be provided with various practical problems, which will help develop confidence in tackling security flaws and breaches in computing systems and using penetration testing tools. The timely constructive feedback during practical lab exercises will support students in developing the skills and knowledge required for the coursework exercise.

The module will be assessed through weekly lab work (5%) and lab tests (25%) taken at regular intervals throughout the semester to evaluate students' skills and practical understanding of the hacking concepts. This will be followed by a coursework exercise (70%) that requires students to design, implement and document penetration tests and mitigation measures to thwart and reduce cyber threats posed to the target system. Students will produce a report detailing their work based on a scenario or case study.

If a student requires supplementary assessment for re-assessment, they will be asked to take a computer-based assessment and carry out penetration tests for a given range of questions based on a particular scenario to demonstrate evidence for the required learning outcomes.

Mode of Assessment

Type	Method	Description	Weighting
Summative	Attendance requirement	An individual mark is allocated to reflect a student?s attendance.	5%
Summative	Computerised examination	Scenario-based questions to test knowledge and understanding of core concepts	25%
Summative	Coursework - Written	Exercises in the development of a secure system using penetration tests. Equivalent to 4000 words.	70%

Reading List

To access the reading list for this module, please visit https://bradford.rl.talis.com/index.html

Please note:
This module descriptor has been published in advance of the academic year to which it applies. Every effort has been made to ensure that the information is accurate at the time of publication, but minor changes may occur given the interval between publishing and commencement of teaching. Upon commencement of the module, students will receive a handbook with further detail about the module and any changes will be discussed and/or communicated at this point.

https://bradford.ac.uk