WM285-15 Security Testing II

27/28

Department
WMG
Level
Undergraduate Level 2
Module leader
Michael Macaulay
Credit value
15
Module duration
10 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Penetration testers and red teams require deep understanding of the underlying technologies, such as network protocols, operating systems, and applications, as well as a range of transferable skills such as project management, team working, report writing and communication. This module covers the latest techniques of ethical hacking and provides practical experience in selecting and applying suitable tools and techniques.
The module is also designed to ensure that students are able to define the scope of testing under certain requirements and develop a relevant project plan, and carry out a security assessment by applying appropriate testing methodologies and tools.further emphasis is given to understanding of the requirements, preparation and reporting of testing results, impact, risk and countermeasures.

Module aims

This module aims to equip students with the advanced knowledge and practical experience of performing professional security assessment, including testing of the organisation's monitoring, detection and response, and reporting to client organisations.
There is a fundamental emphasis on professionalism. Students are given an in-depth knowledge of the phases of a professional security assessment. Participants are made aware of the need to act professionally, in an ethical manner and are made aware of ‘responsible reporting’

programmes.
This module is partly taught by professional practitioners involved with professional penetration testing on a daily basis and also equipped with years of university academic experience.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Understanding Requirements
Defining Scope
Project planning and management
Assessing network design
Assessing application design
Avoiding Detection
Managing Risk
Testing Methodology
Testing Platforms
Technology and Vulnerabilities
Social Engineering

Learning outcomes

By the end of the module, students should be able to:

- Demonstrate a critical understanding of the professional, legal and ethical issues related to ethical hacking and its application in different environments [CITP 2.1.1, 2.1.2]
- Interpret and apply penetration testing methodologies and security assessment tools following on the scope, requirements and technologies of target infrastructure [CITP 2.1.1, 2.1.2, 2.1.4, 3.2.2]
- Evaluate the security posture of a system using an appropriate methodology, and assess potential vulnerabilities related to organisational, policy or technical issues [CITP 2.1.1, 2.1.2, 2.1.4, 3.2.2, 4.2.2]
- Analyse and report the outcomes of a security test to a professional standard, recommending and specifying suitable security controls [CITP 2.1.1, 2.1.2, 2.1.4, 3.2.2, 4.2.2]

Indicative reading list

Reading lists can be found in Talis

Specific reading list for the module

Subject specific skills

Participants will develop advanced system penetration skill, aimed at bypassing advanced security controls and avoiding detection.

Participants will develop hands-on experience of managing a security assessment (red teaming) project from the beginning, elucidating requirements in initial scope agreement and the preparation of a professional report aimed at senior management.

Transferable skills

Planning and project management
Communication and presentation

Study

Study time

Type	Required
Lectures	12 sessions of 1 hour (8%)
Supervised practical classes	18 sessions of 1 hour (12%)
Online learning (independent)	16 sessions of 1 hour (11%)
Other activity	6 hours (4%)
Private study	38 hours (25%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Further practical lab work and research.

Other activity description

NA

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Assessment component			
Portfolio of Knowledge and Skills	70%	42 hours	Yes (extension)
Reassessment component is the same			
Assessment component			
In-Class Test	30%	18 hours	No
Face to face, non open book, in-class test.			
Reassessment component is the same			

Feedback on assessment

Verbal feedback during lab sessions.
Feedback/ marksheets for assessments.
Summative feedback for assessments.

Availability

Courses

Course availability information is based on the current academic year, so it may change.
This module is Core for:

- Year 2 of UWMA-H651 Undergraduate Cyber Security