WM185-15 Security Testing I

25/26

Department
WMG
Level
Undergraduate Level 1
Module leader
Christo Panchev
Credit value
15
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Increasing the robustness and resiliency of systems against threats and attacks is a key cyber security goal. Although, cyber security practitioners should be involved in system design early enough to design cyber-resiliency into the system, quite often, they are presented with legacy systems designed with little consideration to cyber-security. Notwithstanding, even well-designed systems are prone to cyber-attacks from both organised and ill-organised perpetrators.
Penetration testers and red teams must possess a good understanding of network protocols and design. This enables practitioners to gain a basic understanding of the root causes of network vulnerabilities and the associated remedial measures that can be taken, particularly where the root cause relates to network misconfiguration issues (both hardware and protocol related).

Module aims

This module aims to equip students with the knowledge and practical experience of performing security testing and producing professional penetration testing reports for client organisations.
This module begins by introducing the security testing methodologies and relevant process.
Students are given an extensive knowledge of the phases of a penetration test which involve (for example) information gathering (reconnaissance), threat modelling, vulnerability analysis, exploitation. post-exploitation and reporting.
Having gained this fundamental knowledge, students proceed to develop in-depth skills of how to

conduct a professional penetration test on a network.
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.

Network security

- Network security monitoring, passive, proactive, technical, non-technical, consequences;
  Operating system security, web security, embedded security, cloud and virtualisation security, security as a service
  Penetration testing
- Information gathering methods, techniques and tools. Footprinting, reconnaissance, network port scanning.
- Vulnerability exploitation. Gaining and maintaining access, covering tracks, enumeration techniques and vulnerability assessment, static and dynamic analysis of malware, social engineering, SQL injection, and zero-day exploits, session hijacking, denial-of-Service, password cracking, firewalking techniques, evading intrusion detection systems and firewalls, hacking web applications and SQL injection attacks.
- Penetration testing. Professionalism, ethics and responsible reporting; penetrations testing methodologies, standards and plans.

Learning outcomes

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

- Appraise the security posture of a network by analysing the network configuration using appropriate tools where necessary.
- Evaluate the configuration of network security devices to achieve a desired security posture recommending adjustments where appropriate.
- Demonstrate an understanding of vulnerability exploitation techniques.
- Assess the results of system security tests and recommend appropriate mitigation strategies – which may include possible design and configuration changes.

Indicative reading list

Andrew, S., 2011. Tanenbaum, and J. Wetherall. Computer Networks, 5th Edition, Morgan Kaufmann
Baloch, R., 2017. Ethical hacking and penetration testing guide. CRC Press.
Google Hacking for Penetration Testers, Syngress Baloch, R., 2015,
Ethical Hacking and Penetration Testing Guide, CRC Press Svensson, R., 2016,

Subject specific skills

Understanding of system defence and offence principles, strategies, techniques and concepts
Identification, evaluation and exploitation of system vulnerabilities.

Transferable skills

Critical and analytical thinking
problem solving

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours (24%)
Private study	54 hours (36%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Additional lab work and research

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Ethical hacking test	30%	18 hours	No
An online test with a combination of multiple choice and short answer questions.			
Penetration test of a corporate	60%	36 hours	Yes (extension)

	Weighting	Study time	Eligible for self-certification
network			
Participants will be provided with a network specification in the form of a packet tracer network and a virtualised environment comprising of multiple servers. Participants will be required to plan, prepare, execute and report on a penetration test. The report is aimed at stakeholders with varied technical abilities from managers who have strong technical abilities to senior management interested only in an executive summary.			
Presentation on the results and recommendations from the penetration test	10%	6 hours	No
Students are expected to deliver a presentation on the main findings, conclusions and recommendations from the security test carried out, as well as answer question from the interviewers.			

Feedback on assessment

In a feedback form

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security