WM9PF-15 Ethical Hacking

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Christo Panchev
Credit value
15
Module duration
4 weeks
Assessment
Multiple
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 an in-depth understanding of vulnerabilities and attack methodologies. This enables practitioners to gain a critical understanding of the root causes of network and system vulnerabilities and the associated remedial measures that can be taken.

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 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.

There is a fundamental emphasis on professionalism. Students are made aware of the need to act professionally, in an ethical manner and are made aware of ‘responsible reporting’ programmes.

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. Network security monitoring, passive, proactive, technical, non-technical, consequences; Operating system security, web security, embedded security, security as a service
  Penetration testing and red teaming
- 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 and connected systems by analysing the network configuration using appropriate tools where necessary.
- Critically evaluate the configuration of network and endpoint security controls to achieve a desired security posture recommending adjustments where appropriate.
- Demonstrate a comprehensive 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.
Long, J., 2005. Professional Penetration Testing – Creating and Operating a Formal Hacking Lab, Syngress,
Baloch, R., 2015. Google Hacking for Penetration Testers, Syngress
Allen, L. and Cardwell, K., 2016, Advanced Penetration Testing for Highly-Secured Environments, 2nd edition, Packt Publishing

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Subject specific skills

Advanced applied understanding of system defence and offence principles, strategies, techniques and concepts.
Hands-on experience of managing a penetration testing project from the beginning (elucidating requirements) through the development of a professional report aimed at senior management.

Transferable skills

Critical and analytical thinking
Problem solving
Project planning and management
Communication and report writing

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (20%)
Private study	60 hours (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Further practical 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
Penetration test of a corporate network	80%	50 hours

Students will be provided with a virtualised environment simulating a small networked infrastructure. Students 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.

In module test testing the ability to harden network and systems security configuration	20%	10 hours

Students are tested on their understanding of network and systems security configuration. Students will be provided with a network environment which contains multiple faults. They will undertake a sequence of tests on the network and then determine problems with the configuration - making recommendations and changes as appropriate.

Assessment group R

	Weighting	Study time
Penetration test of a corporate network	100%	

Students will be provided with a virtualised environment simulating a small networked infrastructure. Students 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.

Feedback on assessment

Feedback will be provided as annotated commentary within the submitted work. High level feedback will be provided on a standard WMG feedback sheet. Students will have an opportunity to get further feedback and support directly from the module tutor.

Availability

Courses

This module is Core for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)