### *CMT118: Malware Analysis and Vulnerability Assessment*

|  |  |
| --- | --- |
| **School** | Cardiff School of Computer Science and Informatics |
| **Department Code** | COMSC |
| **Module Code** | CMT118 |
| **External Subject Code** | 100366 |
| **Number of Credits** | 20 |
| **Level** | L7 |
| **Language of Delivery** | English |
| **Module Leader** | Dr Georgios Theodorakopoulos |
| **Semester** | Autumn Semester |
| **Academic Year** | 2019/0 |

#### Outline Description of Module

This module aims to provide students with the necessary skills to perform vulnerability assessments at system and network level. We focus on tools and techniques for penetration testing, static and dynamic malware analysis, and social engineering. Specific contexts include network intrusions, web security, and malware spreading.

#### On completion of the module a student should be able to

1. Perform static and dynamic malware analysis to explain the malware’s anatomy, its effects on a system and its spreading behaviour.
2. Identify, evaluate and recommend, with justification, a selection of configurations and countermeasures to reduce the likelihood and impact of potential security attacks.
3. Perform application penetration testing to identify system and network security vulnerabilities and exploit them.
4. Explain how to detect and react to network intrusions.
5. Explain how web browsers are used to exploit vulnerabilities and inject malicious code into web services (e.g. cross-site scripting).
6. Recognize and defend against social engineering attacks.

#### How the module will be delivered

The module employs a combination of theoretical and practical interactive contact sessions, using a study guide, a selection of papers and case studies. It is anticipated that external speakers will also be invited to give the occasional lecture to the students.

#### Skills that will be practised and developed

Critical evaluation of the claims from proponents of new technologies and methodologies,  
product vendors, researchers and consultants.

Research skills in quantitative and qualitative methods.

Report writing, including writing academic and technical reports, which target different audiences.

Innovation and critical thinking.

Rhetoric and argumentation.

Time management.

Reflective practice: the ability to reflect on performance, as a means of instilling the habit of lifelong learning.

#### How the module will be assessed

The module will be assessed with one Coursework (weight: 30%) and one Examination (weight: 70%).

The Coursework will require students to dissect a piece of malicious code and ascertain its structure, behaviour, and purpose. Following this analysis, students will recommend potential countermeasures to the malicious code and evaluate them with respect to their effectiveness in reducing the impact of this piece of malware. In parallel, students will identify security vulnerabilities in a provided application using penetration testing techniques. The deliverable of this Coursework will be a written report that details and justifies the process that students followed and the findings that arose. The Coursework will assess Learning Outcomes LO1, LO2, LO3.

The Examination will be paper-based, and it will cover a broad range of topics addressed in the module on network security (with an emphasis on network intrusions and how to defend against them), web security (with an emphasis on attacks against web browsers), and social engineering attacks and defences. Students will be required to explain and apply these concepts and techniques in various security scenarios. The examination will assess Learning Outcomes LO2, LO4, LO5, LO6.

Students will be provided with reassessment opportunities in line with University regulations.

#### Assessment Breakdown

| **Type** | **%** | **Title** | **Duration(hrs)** |
| --- | --- | --- | --- |
| Examination - Autumn Semester | 70 | Malware Analysis And Vulnerability Assessment | 2 |
| Written Assessment | 30 | Malware Analysis And Vulnerabilities Assessment | N/A |

#### Syllabus content

Introduction to Information Security.

Malicious Software and Viruses

Static analysis of malware anatomy

Dynamic analysis of malware spreading behaviour

System penetration testing – legality, rules of engagement and reporting

Network penetration testing - sniffing, scanning, botnets, DDoS

Computer/Application penetration testing - buffer overflow, SQL injection, XSS attacks

Social Engineering

#### Essential Reading and Resource List

This is a dynamic area, not effectively covered just with textbooks. Therefore, in addition to background reading below, in order to provide most relevant and up-to-date material, required, recommended and further reading will be made available as a set of web resources. Students will be encouraged to add their own. The reading material will be tagged around the following main categories:

* Malware analysis
* Pentesting – network
* Pentesting – system
* Kevin Mitnick (Social Engineering)

In addition, students will be expected to widely research contemporary issues as reflected in appropriate publications.

#### Background Reading and Resource List

1) Penetration Testing: A Hands-On Introduction to Hacking

By Georgia Weidman

No Starch Press

June 2014, 528 pp.

ISBN-13:

9781593275648

**2) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**  
by Michael Sikorski and Andrew Honig

No Starch Press

February 2012, 800 pp.

ISBN-13:

9781593272906

3) The Art of Deception: Controlling the Human Element of Security

Mitnick, Kevin D., and William L. Simon.

John Wiley & Sons, 2011.