Module 38 Cyber Security & Ethical Hacking

Module title	Cyber Security & Ethical Hacking
Module NFQ level (only if an NFQ level can be demonstrated)	8
Module number/reference	BSCH-CSEH
Parent programme(s)	Bachelor of Science (Honours) in Computing Science
Stage of parent programme	Award stage
Semester (semester1/semester2 if applicable)	Semester 2
Module credit units (FET/HET/ECTS)	ECTS
Module credit number of units	5
List the teaching and learning modes	Direct, Blended
Entry requirements (statement of knowledge, skill and competence)	Learners must have achieved programme entry requirements.
Pre-requisite module titles	BSCH-FC, BSCH-DNA
Co-requisite module titles	None
Is this a capstone module? (Yes or No)	No
Specification of the qualifications (academic, pedagogical and professional/occupational) and experience required of staff (staff includes workplace personnel who are responsible for learners such as apprentices, trainees and learners in clinical placements)	Qualified to as least a Bachelor of Science (Honours) level in Computer Science or equivalent and with a Certificate in Training and Education (30 ECTS at level 9 on the NFQ) or equivalent.
Maximum number of learners per centre (or instance of the module)	60
Duration of the module	One Academic Semester, 12 weeks teaching
Average (over the duration of the module) of the contact hours per week	3
Module-specific physical resources and support required per centre (or instance of the module)	One class room with capacity for 60 learners

Analysis of required learning effort		
	Minimum ratio teacher / learner	**Hours**
Effort while in contact with staff		
Classroom and demonstrations	1:60	36
Monitoring and small-group teaching		
Other (specify)		
Independent Learning		
Directed e-learning		
Independent Learning		55
Other hours (worksheets and assignments)		34
Work-based learning – learning effort		
Total Effort		125

Allocation of marks (within the module)					
	Continuous assessment	**Supervised project**	**Proctored practical examination**	**Proctored written examination**	**Total**
Percentage contribution	50%			50%	100%

Module aims and objectives

The module details the cost of breaches and hacks to organizations and hence the importance of ethical hacking and penetration testing. Encryption is covered, from simple classical techniques to modern PK techniques. Learners are shown the process of auditing application source code to verify that the proper security controls are present. The module focusses on web applications. XSS, SQLi, insecure code, code errors.

Other concepts such as steganography, network security (basic analysis of packet captures), and system misconfiguration will be covered.

Minimum intended module learning outcomes

On successful completion of this module, the learner will be able to:

1. Critique encryption, from classical to modern crypto.
1. Defend the concept and implementation of ethical hacking.
2. Analyse and implement state-of-art penetration testing tools.
3. Code and deploy software securely.
4. Apply appropriate security policies.
5. Review code to detect vulnerabilities.

Rationale for inclusion of the module in the programme and its contribution to the overall MIPLOs

In the current social and economic climate, computer security is paramount. Nowadays there is more focus on security and privacy. This module provides a solid foundation for all security topics found in computer science from a theoretical and practical perspective.

Appendix 1 of the programme document maps MIPLOs to the modules through which they are delivered.

Information provided to learners about the module

Learners receive a programme handbook to include module descriptor, module learning outcomes (MIMLO), class plan, assignment briefs, assessment strategy, and reading materials.

Module content, organisation and structure

Basics of Cyber Securit

- Cyber Securityas an ontology
- Policies
- Confidentiality, integrity, availability, and related concepts
- Access control – ACLs, network devices

Encryption

- Classical – Caesar, ROT, Vigenere
- Modern – Private key, public key, Key exchange, DES
- Modern principles - Trapdoor functions, modulo arithmetic
- Modes of operation
- TLS handshake

Ethical Hacking

- Introduction to ethical hacking
- The role of security professionals and penetration testers
- OWASP (Top 10)

Information gathering

- The role of reconnaissance
- Unearthing initial information
- Footprinting and related tools
- Scanning and related tools
- Enumeration and related tools

Module teaching and learning (including formative assessment) strategy

The module is delivered through a series of lectures. The emphasis is on developing knowledge and understanding in context.

Assessment is divided into three elements. The continuous assessment consists of a presentation on a prescribed and a comprehensive report on the same topic. These assess the learner's understanding in specific areas of the syllabus. Finally, there is an end of semester exam that tests the learners understanding of the theoretical material.

Timetabling, learner effort and credit

The module is timetabled as one 3-hour lecture per week.

There are 36 contact hours made up of 12 lectures delivered over 12 weeks with classes taking place in a classroom. The learner will need 55 hours of independent effort to further develop the skills and knowledge gained through the contact hours. An additional 34 hours are set aside for learners to work on worksheets and assignments that must be completed for the module as a part of the continuous assessment.

Work-based learning and practice-placement

There is no work based learning or practice placement involved in the module.

E-learning

The college VLE is used to disseminate notes, advice, and online resources to support the learners. The learners are also given access to Lynda.com as a resource for reference.

Module physical resource requirements

Requirements are for a classroom for 60 learners equipped with a projector.

Reading lists and other information resources

Recommended Text

Simpson, M.T. (2017) *Hands-on Ethical Hacking and Network Defence*. Boston: Cengage Learning

Secondary Reading

Regalado D, et al., (2015) *Grey Hat Hacking*. New York : McGraw-Hill

Recent conference/journal papers related to module topics

Specifications for module staffing requirements

For each instance of the module, one lecturer qualified to at least Bachelor of Science (Honours) in Computer Science or equivalent, and with a Certificate in Training and Education (30 ECTS at level 9 on the NFQ) or equivalent.. Industry experience would be a benefit but is not a requirement.

Learners also benefit from the support of the programme director, programme administrator, learner representative and the Student Union and Counselling Service.

Module Assessment Strategy

The assignments constitute the overall grade achieved, and are based on each individual learner's work. The continuous assessments provide for ongoing feedback to the learner and relates to the module curriculum.

No.	Description	MIMLOs	Weighting
1	**Assignment** Learners are asked to submit a dissertation on a (different) topic related to recent technologies and trends in the field of ethical hacking and security.	1-6	25%
2	**Presentation** Each learner will be asked to prepare a presentation regarding the topic covered in no. 1. Presentation will be short, 5-10 minutes.	1-6	25%
3	Written exam that tests the theoretical aspects of the module.	1-6	50%

All repeat work is capped at 40%.

Sample assessment materials

Note: All assignment briefs are subject to change in order to maintain current content.

Cyber Security & Ethical Hacking

Assignment

25% - Overall

The contents of the encrypted archive file (file.7z) are required. The following message was found attached to the monitor of a computer (IP address is 192.168.0.10) where the file was located:

> “Ilx trhwpsis ml tvcrr”

The above information is obviously encrypted. More information is required.

You have access to the network where the computer is located. How would you examine the network? Write a short paragraph about possible avenues of discovery.

[5 marks]

Go to the online EH tool and run the command to discover information. What information did you uncover?

(The online EH tool is a simulation of a command-line interface)

[5 marks]

What is the decrypted message?

[5 marks]

What are the contents of the decrypted archive file?

[10 marks]

GRIFFITH COLLEGE DUBLIN

QUALITY AND QUALIFICATIONS IRELAND
EXAMINATION

Cyber Security & Ethical Hacking

Lecturers:	**Lee Tobin**
External Examiner:	

Date:	**Time:**

THIS PAPER CONSISTS OF FOUR QUESTIONS
FOUR QUESTIONS TO BE ATTEMPTED
ALL QUESTIONS CARRY EQUAL MARKS

QUESTION 1

[BASICS OF IS]

What is Information Risk Management?

(5 marks)

Explain the difference between the top-down and bottom-up approaches to Cyber Securit.

(5 marks)

Explain the difference between capability lists and access control lists

(5 marks)

What is the bootstrapping problem in the context of security auditing?

(5 marks)

What is the difference between authorisation and authentication?

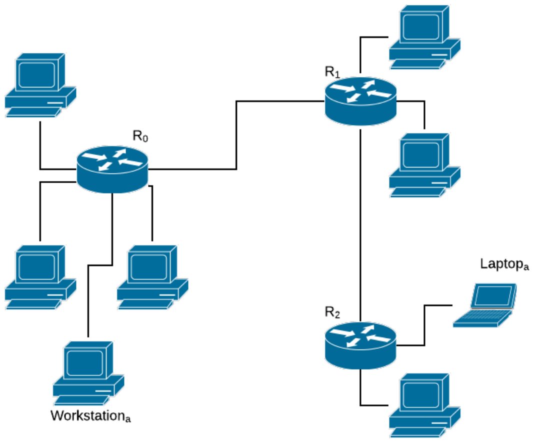
(5 marks)

(Total 25 marks)

QUESTION 2

[NETSEC]

Where would the ***extended*** *ACL* be placed in the following network to prevent Workstation$_a$ from communicating with Laptop$_a$? Use this diagram in your answer, indicating the location and the interface where your ACL is to be placed.



(10 marks)

Briefly explain how the Kerberos authentication protocol works. Try to use diagrams in your explanation.

(15 marks)

(Total 25 marks)

QUESTION 3

[ENCRYPTION]

Given the 2DES/2 encryption scheme:

$C = E_{k2}(E_{k1}(P))$

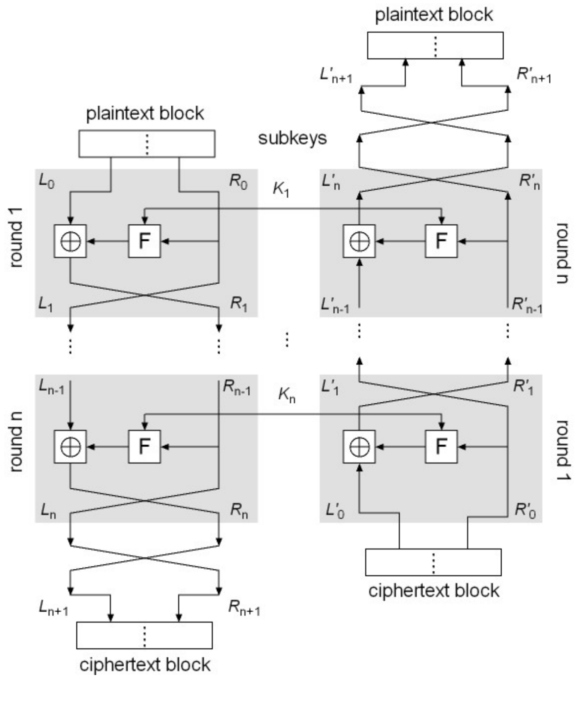
The naïve brute force attack approach is:

$P = D_{k1}(D_{k2}(C))$

Explain how the *meet-in-the-middle* attack works.

(10 marks)

The diagram below outlines the Feistel cipher. Briefly explain how it works.



(15 marks)

(Total 25 marks)

QUESTION 4

[ETHICAL HACKING]

What is the difference between white hat and black hat hacking?

(5 marks)

The following code is vulnerable to what attack?

```
uid = getRequest("UserId");
sql = "SELECT * FROM Users WHERE UserId = " + uid;
```

(5 marks)

Describe how would you perform the attack?

(10 marks)

Describe how you could mitigate this attack?

(5 marks)

(Total 25 marks)