Module Specification

Cyber Security [TSI]

Version: 2023-24, v2.0, 09 Aug 2023

Contents

Part 1: Information

Module title: Cyber Security [TSI]

Module code: UFCE6X-12-3

Level: Level 6

For implementation from: 2023-24

UWE credit rating: 12

ECTS credit rating: 6

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: Transport and Telecommunication Institute

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Not applicable

Features: Not applicable

Educational aims: Provide an in-depth, theoretical understanding of network security. Provide students with the knowledge and skills necessary to design and support network security.

Outline syllabus: •Modern Network Security Threats
•Securing Network Devices
•Authentication, Authorization and Accounting
•Implementing Firewall Technologies
•Implementing Intrusion Prevention
•Securing the Local Area Network
•Cryptography
•Managing a Secure Network

Part 3: Teaching and learning methods

Teaching and learning methods: Learning and teaching will be provided to students in two forms: lectures and labs. During lectures, theoretical aspects of the course will be provided to students by the teaching staff. Lectures will be supported by presentation published and available to the students on e.tsi.lv under the module section. Also, additional materials, like text books, publications on the internet, videos etc will be presented in e.tsi.lv.
During labs, each student receives an individual task to perform

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Critically analyses and evaluate modern types of threats and attacks. Research common tools and procedures which could mitigate the impact, evaluating their effectiveness.

MO2 Explain how network-based Intrusion Prevention Systems (IPS) are used to help secure a network. Explain endpoint vulnerabilities and protection methods.

MO3 Evaluate the different approaches commonly applied by medium/large sized enterprises to achieve Confidentiality, Integrity and Authentication.

MO4 Apply an in-depth understanding and knowledge of modern network security principles, limitations and configurations applicable for a small/medium size enterprise.

Hours to be allocated: 120

Contact hours:

Independent study/self-guided study = 96 hours

Face-to-face learning = 64 hours

Total = 160

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/0F6BDD86-3E2A-AD41-4B0E-CF9C28C49506.html?lang=en&login=1

Part 4: Assessment

Assessment strategy: This module will include a range of formative and summative assessments.

The module will follow the CISCO syllabus and a series of MCQ tests will be completed at the end of each chapter to allow students to track their understanding.

Students will complete 2 practical skills assessments, 1. design and implement, 2. reconfigure following finds of the report.

Students will be required to complete a written report. This report should investigate the threat landscape, reviewing the tools and techniques which are commonly adopted / employed by campaign groups to attack network. This report should review the effectiveness of the current standards and regulations and suggest recommendations on improvements.

Resits will be like for like.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: Practical assessment design and implement.
Weighting: 25 %

Final assessment: No
Group work: No
Learning outcomes tested: MO4

Practical Skills Assessment (First Sit)
Description: Practical assessment apply and document security configurations.
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO4

Written Assignment (First Sit)
Description: Detailed report (3000 words) describing an overview of threat landscape and current security practices.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Practical Skills Assessment (Resit)
Description: Detailed report describing an overview of threat landscape and current security practices.
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO4

Practical Skills Assessment (Resit)
Description: Practical assessment design and implement.
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO4

Written Assignment (Resit)
Description: Detailed report (3000 words) describing an overview of threat landscape and current security practices.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Computer Science and Software Development {Double Degree} [Feb][FT][TSI][4yrs] BSc (Hons) 2020-21

Computer Science and Software Development {Double Degree} [Oct][FT][TSI][4yrs] BSc (Hons) 2020-21