Unit Title	Ethical Hacking and Digital Forensics (blended)
FHEQ Level	Level 5
Unit Code	CYS20206
Credit Value	30
Unit Type	Subject

Learning Hours (Blended)			
Staff – Student Contact Hours		**Independent Study Hours**	
Classes	45	Independent study	195
Supervised access to Ravensbourne resources	30	Preparation for assessment	30
Total		300	

Unit Description

This unit introduces students to basic principles of Ethical Hacking and Digital Forensics.

Ethical Hacking or penetration testing provides an insight into effectiveness of security measures in place for digital infrastructure and to reinforce the existing mechanisms. The purpose of this process is to identify any vulnerabilities and weaknesses in the system and to protect against unauthorised access. The outcome of this process results in applying preventive or corrective measures to mitigate the identified risks.

The unit will also develop understanding of cyber-crime and forensic analysis of various digital devices including mobile and cloud along with various techniques to look at the evidence and presenting it with legal perspective.

The Five Principles underpin the Mindsets and Skillsets Manifesto and are the foundation upon which all course curriculum frameworks and unit specifications are based. The relevant Principles as stated below have been mapped against the Learning Outcomes relevant to each course unit and at each level (see Programme Specifications for full description of the Five Principles):

1. Cultivate / Where the individual thrives.
2. Collaborate / Where disciplines evolve.
3. Integrate / Where education engages industry.
4. Advocate / Where purpose meets practice.
5. Originate / creativity meets technology.

Unit Indicative Content

Ethical Hacking and Digital Forensics

Industry-wide Knowledge

- Cyber Crime and Digital Evidence
- Digital Forensics Process (Identification, collection, examination, analysis, presentation)
- Forensics: Conceptual Models
- Storage, Memory and Cloud Forensics
- Penetration Testing Fundamentals
- Hardware Analysis
- External and internal inspection
- UART Communications, I2C and SPI
- JTAG debugging
- Firmware reverse engineering
- Exploiting IoT, mobile, web and local network
- Software defined radio
- Zigbee and BLE
- WiFi and network monitoring
- Cryptography
- WireShark,Web hacking and SQL Injection
- Vulnerability Scanning
- Kali Linux

AWS Specific Knowledge Area

- Cloud Forensics
- Fortinet FortiAnalyzer-VM Centralized Security Logging and Reporting
- Sophos UTM 9 (PAYG)
- AccessData Lab

CyBOK knowledge areas

- Digital Forensics

Unit Aims

1. To analyse and Identify potential security threats to digital infrastructure and content
2. To apply penetration testing techniques
3. To apply digital forensics knowledge in a given case study or scenario keeping in view the legal and professional guidelines
4. To develop an understanding of test plans
5. To provide potential solutions to overcome identified vulnerabilities in a system
6. To evaluate the processes and procedures for carrying out digital Forensic Investigation.

Unit Learning Outcomes

LO 1 Research/Inspiration

Analyse and interpret information gathering techniques using a wide range of sources, providing visual, contextual and industry case-study research as appropriate.

Related Principle: ORIGINATE

LO 5 Presentation /Storytelling for Influence

Select and employ effective methods of presentation and communication of projects in considering the audience/client and the purpose of the work, whether in visual, oral or written form.

Related Principle: ADVOCATE

LO 6 Critical and creative mindsets Analyse conceptions of diverse practice and use this to inform a course of action

Related Principle: ORIGINATE

LO 8 Professional Identity
Investigate specific professional contexts to situate your own practice
Related Principle: CULTIVATE

Learning and Teaching Methods

This unit will be delivered using a combination of:

- Lectures / Seminars
- Online activities
- Self-directed independent study
- Peer learning, group discussion, guest speakers

Assessment methods and tasks	
Assessment tasks	**Weighting (%)** *(one grade or multi-grade unit)*
Project portfolio	40% (holistic)
Online test	30%
Practical assessment (15 minutes)	30%

Indicative Assessment Criteria

With the help of appropriate tools, analyse and Identify potential security threats to digital infrastructure and content, provide possible solutions to identified problems (LO1, LO6)

Apply penetration testing techniques to a given situation (LO8)

Apply digital forensics knowledge in a given case study or scenario keeping in view the legal and professional guidelines (LO8)

Apply the knowledge gained during this module using tools for a digital forensic investigation with a test plan (LO5)

Demonstrate the processes and procedures for carrying out digital Forensic Investigation. (LO6)

Essential Reading list

The Cyber Security Body of Knowledge. (2019). 1st ed. The National Cyber Security Centre.

Gregg, Michael C.. Certified Ethical Hacker (CEH) Version 9 Cert Guide. Pearson., 2017.

Årnes, A. (2018). Digital forensics. 1st ed. Wiley.

Recommended Reading List

Easttom, C. (2018). Network defense and countermeasures. Indianapolis, Indiana: Pearson.

Easttom, C. (2018). Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits (Pearson IT Cybersecurity Curriculum (ITCC)). Pearson.

Kävrestad, Joakim. Fundamentals of Digital Forensics Theory, Methods, and Real-Life Applications. Springer International Publishing, 2018.

Same as Networking and Cyber Security Modules

Further reading and resources will be identified in your Project Brief.