Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM764
Module Title	Offensive Security and Incident Response
Level	7
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GCAP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc Cyber Security	Core
MSc Cyber Security with Advanced Practice	Core

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	10 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	11 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**21** hrs
Placement / work based learning	0 hrs
Guided independent study	179 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2024
Date and details of revision	
Version number	1

Module aims

This module is designed to equip students with a comprehensive understanding of offensive security techniques and incident response strategies. This module focuses on practical aspects such as penetration testing, vulnerability assessment, and ethical hacking, enabling students to simulate real-world cyberattacks. By engaging in hands-on activities, students will develop practical skills in identifying vulnerabilities within systems and networks. Furthermore, they will learn how to respond to security incidents effectively, enhancing their ability to mitigate risks and safeguard against potential threats. This module empowers students to proactively address security challenges and contribute to maintaining robust cybersecurity measures.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Apply offensive security techniques, including vulnerability assessments and penetration testing.
2	Implement incident response strategies to effectively detect, analyse, and respond to security incidents.
3	Evaluate and mitigate security risks by identifying vulnerabilities and implementing appropriate countermeasures.
4	Critically evaluate offensive security tools, frameworks, and methodologies to assess the security posture of systems and networks effectively.
5	Demonstrate the ability to clearly communicate findings, recommendations, and incident response actions to technical and non-technical stakeholders

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment of this module is based on a portfolio approach, providing students with an opportunity to showcase their skills, knowledge, and understanding of offensive security techniques and incident response strategies. The portfolio assessment will consist of a collection of artefacts that demonstrate the students' proficiency in conducting penetration testing, vulnerability assessments, and ethical hacking activities. It will also include evidence of their ability to effectively detect, analyse, and respond to security incidents following established frameworks and best practices. The portfolio may include reports, vulnerability assessment findings, incident response plans, documented exploits, and reflective journals. This assessment approach allows for a comprehensive evaluation of students' capabilities, encourages critical thinking and problem-solving skills, and provides an opportunity for self-reflection and improvement. It also aligns with industry practices, as professionals in

offensive security and incident response often compile portfolios to showcase their expertise.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4,5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Offensive Security principles
- Ethical Hacking
- Penetration Testing Methodologies
- Vulnerability Assessment and Scanning
- Exploitation Techniques and Post-Exploitation
- Web Application Security and Attacks
- Wireless Network Security and Attacks
- Incident Response
    - Detection and Analysis
    - Containment and Eradication
    - Recovery

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

Gerard Johansen, *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response*, 3rd Edition. Gerard Johansen, Packt Publishing 2022

Other indicative reading

O. Santos, *Cisco CyberOps Associate 200-201.* Omar Santos, Cisco Press, 2021.

R. Martinez, *Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting*, Packt Publishing, 2022.

D. Stuttard & M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Indianapolis, IN: Wiley, 2011.

M. Sikorski & A. Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. San Francisco, CA: No Starch Press, 2012.

D. Murdoch, T. Crothers & J. Healey, *Blue Team Handbook: Incident Response Edition.* CreateSpace Independent Publishing Platform, 2012.

M.H Ligh, A. Case, J. Levy & A. Walters, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Indianapolis, IN: Wiley, 2014.

J. Erickson, *Hacking: The Art of Exploitation* (2nd ed.). San Francisco, CA: No Starch Press, 2008.

S. Davidoff & J. Ham, *Network Forensics: Tracking Hackers through Cyberspace*. Upper Saddle River, NJ: Prentice Hall, 2012.