INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» iyul

INTERNATIONAL QUALIFICATIONS AND ASSESSMENT CENTRE
XALQARO MALAKALAR VA BAHOLASH MARKAZI
IQAC

Programme	**CYBER SECURITY DIPLOMA - LEVEL 6**		
Unit Number/ Unit Title	**UNIT 6 CAPSTONE PROJECT**		
Cohort Code:	L06CPAC-U6		
Unit Level	Level 6		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	10 CATS/ 5 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This capstone module provides learners the opportunity to integrate and apply knowledge from previous units to a substantial cyber security project. It enables students to investigate real-world problems, propose evidence-based solutions, and demonstrate critical thinking, innovation, and professional practice in the field of cyber security.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:- 1. Progressive tasks 2. Digital resources

	3. Verbal support 4. Variable outcomes 5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials** • Creswell, J. (2018). Research Design: Qualitative, Quantitative and Mixed Methods. Sage. • Gregory, P. (2023). CISSP Guide to Security Strategy. McGraw-Hill. • Yin, R. (2017). Case Study Research and Applications. Sage Publications. • British Computer Society (BCS). Code of Conduct & Ethics. • OWASP Foundation. Security Project Best Practices.

Learning Outcome	Assessment Criteria
LO1. Formulate a research or industry problem in cyber security.	**Proposal Document:** 1.1 Define clear research or project objectives aligned with cyber security domains. 1.2 Justify the significance and scope of the problem.
LO2. Apply appropriate methodologies and tools for problem-solving.	**Project Report:** 2.1 Use technical and theoretical approaches to investigate the problem. 2.2 Document tools, experiments, or simulations used.
LO3. Analyse data, synthesize findings, and develop actionable insights.	**Technical Portfolio:** 3.1 Interpret data/evidence using critical analysis. 3.2 Recommend practical or strategic solutions based on findings.
LO4. Demonstrate project management, documentation, and communication skills.	Viva + Progress Logs: 4.1 Maintain project timelines, logs, and meeting records. 4.2 Deliver a professional verbal presentation and defend work.
LO5. Reflect on professional practice and ethical considerations.	Reflective Essay: 5.1 Evaluate personal and professional learning. 5.2 Discuss ethical and legal constraints encountered during the project.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Identifying Cybersecurity Research Gaps**	**Identifying Cybersecurity Research Gaps** – Trends, challenges, and emerging threats.	LO1: Formulate a research or industry problem in cybersecurity.	
2	**Defining Project Objectives**	**Defining Project Objectives** – Aligning with domains (e.g., network security, ethical hacking, AI in cybersecurity).	LO1: Formulate a research or industry problem in cybersecurity.	
3	**Problem Justification & Scope**	**Problem Justification & Scope** – Industry relevance, impact, and constraints.	LO1: Formulate a research or industry problem in cybersecurity.	
4	**Literature Review & Background Research**	**Literature Review & Background Research** – Analyzing existing studies and reports.	LO1: Formulate a research or industry problem in cybersecurity.	
5	**Stakeholder & Requirement Analysis**	**Stakeholder & Requirement Analysis** – Identifying target audiences (businesses, governments, end-users).	LO1: Formulate a research or industry problem in cybersecurity.	
6	**Proposal Writing & Approval**	**Proposal Writing & Approval** – Structuring a formal project proposal.	LO1: Formulate a research or industry problem in cybersecurity.	
7	**Research Methodologies in Cybersecurity**	**Research Methodologies in Cybersecurity** – Qualitative vs. quantitative approaches.	LO2: Apply appropriate methodologies and tools for problem-solving.	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	

9	**Threat Modeling & Risk Assessment Techniques**	**Threat Modeling & Risk Assessment Techniques** – STRIDE, DREAD, MITRE ATT&CK.	LO2: Apply appropriate methodologies and tools for problem-solving.	
10	**Tools for Cybersecurity Investigations**	**Tools for Cybersecurity Investigations** – Wireshark, Metasploit, Nmap, SIEM solutions.	LO2: Apply appropriate methodologies and tools for problem-solving.	
11	**Simulating Cyberattacks & Defenses**	**Simulating Cyberattacks & Defenses** – Penetration testing, vulnerability scanning.	LO2: Apply appropriate methodologies and tools for problem-solving.	
12	**Data Collection & Experimentation**	**Data Collection & Experimentation** – Log analysis, malware behavior studies.	LO2: Apply appropriate methodologies and tools for problem-solving.	
13	**Documenting Technical Processes**	**Documenting Technical Processes** – Lab reports, tool configurations, code snippets.	LO2: Apply appropriate methodologies and tools for problem-solving.	
14	**Review**	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	**Midterm**	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		
16	**Feedback & Reflection**	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Data Analysis Techniques**	**Data Analysis Techniques** – Statistical, behavioral, and forensic analysis.	LO3: Analyze data, synthesize findings, and develop actionable insights.	

18	**Identifying Attack Patterns & Anomalies**	**Identifying Attack Patterns & Anomalies** – Correlating evidence from logs/traces.	LO3: Analyze data, synthesize findings, and develop actionable insights.	
19	**Comparative Analysis of Security Solutions**	**Comparative Analysis of Security Solutions** – Firewalls, IDS/IPS, encryption methods.	LO3: Analyze data, synthesize findings, and develop actionable insights.	
20	**Developing Mitigation Strategies**	**Developing Mitigation Strategies** – Patching, policies, awareness training.	LO3: Analyze data, synthesize findings, and develop actionable insights.	
21	**Cost-Benefit Analysis of Security Measures**	**Cost-Benefit Analysis of Security Measures** – ROI for proposed solutions.	LO3: Analyze data, synthesize findings, and develop actionable insights.	
22	**Finalizing Technical Recommendations**	**Finalizing Technical Recommendations** – Executive summaries for stakeholders.	LO3: Analyze data, synthesize findings, and develop actionable insights.	
23	**Review**	**Agile & Waterfall Project Management** – Sprint planning, milestones, deliverables.		
24	**Maintaining Progress Logs & Version Control**	**Maintaining Progress Logs & Version Control** – Git, project diaries, meeting minutes.	LO4: Demonstrate project management, documentation, and communication skills.	
25	**Writing the Final Project Report**	**Writing the Final Project Report** – Structure, citations, and professional formatting.	LO4: Demonstrate project management, documentation, and communication skills.	
26	**Preparing a Professional Presentation**	**Preparing a Professional Presentation** – Slides, demos, and public speaking practice.	LO4: Demonstrate project management, documentation, and communication skills.	
27	**Viva Voce & Project Defense**	**Viva Voce & Project Defense** – Handling Q&A, justifying methodologies.	LO4: Demonstrate project management, documentation, and communication skills.	

28	**Personal Skill Development Review**	**Ethical & Legal Reflections** – GDPR, HIPAA, responsible disclosure dilemmas. **Personal Skill Development Review** – Technical growth, teamwork, time management. **Lessons Learned & Future Improvements** – Project limitations and scalability.	LO5: Reflect on professional practice and ethical considerations.	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	