INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «___» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 7**		
Unit Number/ Unit Title	**UNIT 4 ETHICAL HACKING, RED/BLUE TEAMING, AND CYBER WARFARE SIMULATION**		
Cohort Code:	L07EHRB-U4		
Unit Level	Level 7		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This unit equips learners with advanced offensive and defensive cyber skills through real-world cyber warfare simulations. Students will gain hands-on experience in ethical hacking, red teaming, blue teaming, and the design of cyber ranges and exercises. Emphasis is placed on ethical, legal, and tactical dimensions of modern cyber conflict.
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** • Grimes, R. A. (2017). Hacking the Hacker. Wiley. • Allen, J. (2020). Offensive Countermeasures: The Art of Active Defense. • MITRE ATT&CK Framework Documentation. • Greenberg, A. (2019). Sandworm: A New Era of Cyberwar. • EC-Council. Certified Ethical Hacker v11 Courseware.

Learning Outcome	Assessment Criteria
LO1. 1. Apply advanced ethical hacking methodologies.	1.1 Conduct multi-layered penetration tests using tools (e.g., Metasploit, Burp Suite). 1.2 Demonstrate post-exploitation techniques in controlled environments.
LO2. 2. Develop red team operations.	2.1 Design realistic red team campaigns targeting organizational systems. 2.2 Evaluate tactics, techniques, and procedures (TTPs) using ATT&CK Matrix.
LO3. 3. Execute blue team defense strategies.	3.1 Configure SIEM tools and incident response playbooks. 3.2 Analyze red team engagements and develop countermeasures.
LO4. **4. Simulate cyber warfare scenarios.**	4.1 Create cyber range environments using virtualization/emulation. 4.2 Orchestrate attack-defense exercises aligned with real- world APT profiles.
LO5. 5. Evaluate legal and ethical considerations in offensive security.	5.1 Interpret legal frameworks governing penetration testing and red teaming. 5.2 Discuss ethical dilemmas in state-sponsored cyber operations.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Advanced Penetration Testing Frameworks**	**Advanced Penetration Testing Frameworks** – MITRE ATT&CK, PTES, OSSTMM	LO1: Apply advanced ethical hacking methodologies	
2	**Network Penetration Testing**	**Network Penetration Testing** – VLAN hopping, DNS spoofing, and MITM attacks	LO1: Apply advanced ethical hacking methodologies	
3	**Web App Hacking**	**Web App Hacking** – OWASP Top 10 exploitation (SQLi, XSS, CSRF) with Burp Suite	LO1: Apply advanced ethical hacking methodologies	
4	**Post-Exploitation Techniques**	**Post-Exploitation Techniques** – Privilege escalation, lateral movement, persistence	LO1: Apply advanced ethical hacking methodologies	
5	**Wireless & IoT Hacking**	**Wireless & IoT Hacking** – WPA3 cracking, RFID cloning, SDR attacks	LO1: Apply advanced ethical hacking methodologies	
6	**Lab: Full-Scope Penetration Test**	**Lab: Full-Scope Penetration Test** – From reconnaissance to exfiltration	LO1: Apply advanced ethical hacking methodologies	
7	**Red Team Planning & Scoping**	**Red Team Planning & Scoping** – Objectives, rules of engagement, stealth tactics	LO2: Develop red team operations	
8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Adversary Emulation**	**Adversary Emulation** – Mimicking APT groups (e.g., APT29, Lazarus)	LO2: Develop red team operations	
10	**Custom Malware & C2 Frameworks**	**Custom Malware & C2 Frameworks** – Cobalt Strike, Mythic, Sliver	LO2: Develop red team operations	

11	**Bypassing Modern Defenses**	**Bypassing Modern Defenses** – EDR evasion, AMSI bypass, anti-forensics	LO2: Develop red team operations	
12	**Lab: Red Team vs. Enterprise AD Environment**	**Lab: Red Team vs. Enterprise AD Environment** – Kerberoasting, Golden Ticket attacks	LO2: Develop red team operations	
13	**Debriefing & Reporting**	**Debriefing & Reporting** – TTP documentation and gap analysis	LO2: Develop red team operations	
14	**Review**	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	**Midterm**	- **Final-term assessment** covering all learning outcomes (theory and practical elements)		
16	**Feedback & Reflection**	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**SIEM Configuration & Tuning**	**SIEM Configuration & Tuning** – Splunk, ELK, Microsoft Sentinel	LO3: Execute blue team defense strategies	
18	**Threat Hunting with YARA/Sigma Rules**	**Threat Hunting with YARA/Sigma Rules** – Proactive IOC detection	LO3: Execute blue team defense strategies	
19	**Incident Response Playbooks**	**Incident Response Playbooks** – NIST SP 800-61, SANS PICERL	LO3: Execute blue team defense strategies	
20	**Deception Technologies**	**Deception Technologies** – Honeypots, canary tokens, honey accounts	LO3: Execute blue team defense strategies	
21	**Lab: Analyzing Red Team Logs**	**Lab: Analyzing Red Team Logs** – Detecting covert C2 channels	LO3: Execute blue team defense strategies	

22	**Tabletop Exercise: APT Incident Response**	**Tabletop Exercise: APT Incident Response**	LO3: Execute blue team defense strategies	
23	**Review**	**Cyber Range Design** – Building virtualized attack/defense labs (CLARK, DETER)	LO4: Simulate cyber warfare scenarios	
24	**APT Simulation Exercises**	**APT Simulation Exercises** – Emulating nation-state threats (e.g., Stuxnet, NotPetya)	LO4: Simulate cyber warfare scenarios	
25	**Critical Infrastructure Attacks**	**Critical Infrastructure Attacks** – ICS/SCADA exploitation (Modbus, Siemens)	LO4: Simulate cyber warfare scenarios	
26	**War Game: Capture the Flag (CTF) with Red vs. Blue Teams**	**War Game: Capture the Flag (CTF) with Red vs. Blue Teams**	LO4: Simulate cyber warfare scenarios	
27	**Legal Frameworks for Offensive Security**	**Legal Frameworks for Offensive Security** – CFAA, GDPR, penetration testing contracts	LO5: Evaluate legal and ethical considerations	
28	**Ethics of Cyber Warfare**	**Ethics of Cyber Warfare** – Geneva Convention debates, hack-back policies	LO5: Evaluate legal and ethical considerations	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	