INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «____» _____

Programme	**LEVEL 5 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 8 ETHICAL HACKING AND PENETRATION TESTING**		
Cohort Code:	L05EHPT-U8		
Unit Level	Level 5		
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	To provide students with comprehensive knowledge and practical skills in ethical hacking and penetration testing, enabling them to identify, exploit, and mitigate security vulnerabilities in computer systems and networks. This course emphasizes hands-on experience with various tools and techniques used by ethical hackers to enhance the security posture of organizations.
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** • "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto. • "Hacking: The Art of Exploitation" by Jon Erickson. • "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni.

Learning Outcome	Assessment Criteria
LO1. Understand the principles and legal aspects of ethical hacking and penetration testing.	**1. Written Assessments:** 1.1 Explain the key principles and objectives of ethical hacking. 1.2 Describe the legal and ethical considerations involved in penetration testing. 1.3 Identify the roles and responsibilities of an ethical hacker.
LO2. 2. Develop skills in reconnaissance and information gathering.	**2. Practical Assessments:** 2.1 Conduct passive and active reconnaissance on target systems. 2.2 Use various tools to gather information about network and system vulnerabilities. 2.3 Document and report findings from the information gathering phase.
LO3. 3. Perform vulnerability analysis and exploitation.	**3. Practical Assessments:** 3.1 Identify and analyze vulnerabilities in computer systems and networks. 3.2 Use exploitation tools and techniques to demonstrate vulnerabilities. 3.3 Assess the impact of identified vulnerabilities on system security.
LO4. 4. Develop skills in post-exploitation and reporting.	**4. Practical Assessments:** 4.1 Execute post-exploitation techniques to maintain access and cover tracks. 4.2 Develop comprehensive penetration testing reports. 4.3 Provide recommendations for mitigating identified vulnerabilities.
LO5. 5. Develop skills in post-exploitation and reporting.	**5. Research and Analysis Assessments:** 5.1 Research and analyze various defensive security measures. 5.2 Implement preventive measures to secure systems against attacks. 5.3 Evaluate the effectiveness of different security strategies and controls.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Ethical Hacking**	**Introduction to Ethical Hacking** Definition, objectives, and the hacker mindset	LO1: Foundations of Ethical Hacking	
2	**Legal & Ethical Considerations**	**Legal & Ethical Considerations** Laws (CFAA, GDPR), penetration testing contracts, scope agreements	LO1: Foundations of Ethical Hacking	
3	**Roles & Responsibilities**	**Roles & Responsibilities** Certified Ethical Hacker (CEH), OSCP, red team vs. blue team	LO1: Foundations of Ethical Hacking	
4	**Penetration Testing Methodologies**	**Penetration Testing Methodologies** PTES (Penetration Testing Execution Standard), NIST SP 800-115	LO1: Foundations of Ethical Hacking	
5	**Setting Up a Lab Environment** Kali	**Setting Up a Lab Environment** Kali Linux, Metasploitable, VirtualBox/VMware	LO1: Foundations of Ethical Hacking	
6	**Passive Reconnaissance**	**Passive Reconnaissance** WHOIS, DNS enumeration (nslookup, dig), Google Dorking	LO2: Reconnaissance & Information Gathering	
7	**Active Reconnaissance**	**Active Reconnaissance** Nmap scanning (stealth, aggressive), OS fingerprinting	LO2: Reconnaissance & Information Gathering	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Social Engineering Techniques**	**Social Engineering Techniques** Phishing	LO2: Reconnaissance & Information Gathering	

		simulations, pretexting, OSINT (Maltego)		
10	**Vulnerability Scanning**	**Vulnerability Scanning** Nessus, OpenVAS, Nikto for web apps	LO2: Reconnaissance & Information Gathering	
11	**Documentation & Reporting**	**Documentation & Reporting** Note-taking (KeepNote, Dradis), evidence collection	LO2: Reconnaissance & Information Gathering	
12	**Common Vulnerabilities**	**Common Vulnerabilities** OWASP Top 10 (SQLi, XSS, CSRF), CVE database	LO3: Vulnerability Analysis & Exploitation	
13	**Exploitation Tools**	**Exploitation Tools** Metasploit Framework, Burp Suite, SQLmap	LO3: Vulnerability Analysis & Exploitation	
14	Final Exam Preparation & 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	**Privilege Escalation**	**Privilege Escalation** Windows (Mimikatz), Linux (SUID, kernel exploits)	LO3: Vulnerability Analysis & Exploitation	
18	**Network Exploitation**	**Network Exploitation** Man-in-the-Middle (MITM) attacks, ARP spoofing (Ettercap)	LO3: Vulnerability Analysis & Exploitation	
19	**Web Application Hacking**	**Web Application Hacking** Session hijacking, brute force attacks (Hydra)	LO3: Vulnerability Analysis & Exploitation	

20	**Maintaining Access**	**Maintaining Access** Persistence (backdoors, rootkits), tunneling (Ngrok)	LO4: Post-Exploitation & Reporting	
21	**Covering Tracks**	**Covering Tracks** Log cleaning (eventvwr, /var/log), file wiping	LO4: Post-Exploitation & Reporting	
22	**Penetration Testing Reports**	**Penetration Testing Reports** Structure: Executive summary, technical findings, risk ratings	LO4: Post-Exploitation & Reporting	
23	Review	**Project** Full penetration test on a mock network with report	LO4: Post-Exploitation & Reporting	
24	**Mitigation Strategies**	**Mitigation Strategies** Patch management, WAF rules, secure coding practices	LO4: Post-Exploitation & Reporting	
25	**Client Debriefing**	**Client Debriefing** Presenting findings to stakeholders, remediation timelines	LO4: Post-Exploitation & Reporting	
26	**Defensive Measures**	**Defensive Measures** Honeypots, deception technologies, EDR solutions	LO5: Defensive Security & Research	
27	**Threat Intelligence**	**Threat Intelligence** MITRE ATT&CK framework, TTPs (Tactics, Techniques, Procedures)	LO5: Defensive Security & Research	
28	**Emerging Threats**	**Emerging Threats** AI-powered attacks, zero-day vulnerabilities	LO5: Defensive Security & Research	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	