INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» VI

Programme	**LEVEL 5 EXTENDED DIPLOMA IN CYBERSECURITY**		
Unit Number/ Unit Title	**UNIT 7 ADVANCED NETWORK SECURITY**		
Cohort Code:	L05ANS-U7		
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 advanced knowledge and skills in network security, focusing on securing network infrastructure, detecting and mitigating threats, and ensuring data integrity and confidentiality. Key areas of study include encryption, authentication, authorization, network security architecture, and incident response techniques.
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** • “Network Security Essentials: Applications and Standards" by William Stallings. • "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner. • "Computer and Network Security Essentials" by Kevin Daimi.

Learning Outcome	Assessment Criteria
LO1. 1 Understand advanced network security concepts and principles.	**1. Written Assessments:** 1.1 Explain advanced concepts, terminologies, and principles of network security. 1.2 Identify and describe various types of network threats and vulnerabilities. 1.3 Demonstrate knowledge of encryption, authentication, and authorization mechanisms.
LO2. 2. Develop skills to design and implement secure network architectures.	**2. Practical Assessments:** 2.1 Design a secure network architecture incorporating firewalls, IDS/IPS, and VPNs. 2.2 Implement security measures in a simulated network environment. 2.3 Evaluate the effectiveness of different network security configurations.
LO3. 3. Analyze and respond to network security incidents.	**3. Case Study Assessments:** 3.1 Analyze case studies of network security breaches and identify root causes. 3.2 Develop incident response plans and procedures. 3.3 Assess the impact of security incidents on network infrastructure and data integrity.
LO4. 4. Critically evaluate current trends and emerging technologies in network security.	**4. Research and Analysis Assessments:** 4.1 Conduct research on current trends and emerging technologies in network security. 4.2 Critically analyze the potential impact of new technologies on network security practices. 4.3 Present findings in a well-structured research paper or presentation.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Network Security Principles**	**Network Security Principles** Zero Trust Architecture (ZTA), defense-in-depth	LO1: Advanced Network Security Concepts	
2	**Advanced Encryption Mechanisms**	**Advanced Encryption Mechanisms** IPsec, TLS 1.3, quantum-resistant cryptography	LO1: Advanced Network Security Concepts	
3	**Authentication & Authorization**	**Authentication & Authorization** RADIUS/TACACS+, OAuth 2.0, biometric authentication	LO1: Advanced Network Security Concepts	
4	**Emerging Network Threats**	**Emerging Network Threats** AI-driven attacks, IoT botnets, 5G vulnerabilities	LO1: Advanced Network Security Concepts	
5	**Vulnerability Assessment**	**Vulnerability Assessment** CVSS scoring, penetration testing frameworks	LO1: Advanced Network Security Concepts	
6	**Secure Network Architecture**	**Secure Network Architecture** Segmentation (micro/macro), VLANs, SDN security	LO2: Secure Network Design & Implementation	
7	**Next-Gen Firewalls (NGFW)**	**Next-Gen Firewalls (NGFW)** Deep packet inspection, application-aware filtering	LO2: Secure Network Design & Implementation	
8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**IDS/IPS Configuration**	**IDS/IPS Configuration** Snort rules, Suricata, anomaly-based detection	LO2: Secure Network Design & Implementation	

10	**VPN Technologies**	**VPN Technologies** Site-to-site/IPsec, SSL VPNs, WireGuard	LO2: Secure Network Design & Implementation	
11	**Cloud Network Security**	**Cloud Network Security** AWS Security Groups, Azure NSGs, SASE architecture	LO2: Secure Network Design & Implementation	
12	**Network Forensics**	**Network Forensics** Packet capture analysis (Wireshark, tcpdump)	LO3: Incident Analysis & Response	
13	**Incident Response Frameworks**	**Incident Response Frameworks** NIST SP 800-61, MITRE ATT&CK for networks	LO3: Incident Analysis & Response	
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	**Case Study: Major Breaches**	**Case Study: Major Breaches** SolarWinds, Colonial Pipeline, Equifax	LO3: Incident Analysis & Response	
18	**Threat Hunting**	**Threat Hunting** Proactive detection with SIEM (Splunk, ELK)	LO3: Incident Analysis & Response	
19	**Disaster Recovery**	**Disaster Recovery** Network redundancy, RTO/RPO planning	LO3: Incident Analysis & Response	
20	**AI in Network Security**	**AI in Network Security** Threat detection, automated response (SOAR)	LO4: Trends & Emerging Technologies	

21	**Blockchain for Network Security**	**Blockchain for Network Security** Decentralized identity, DDoS mitigation	LO4: Trends & Emerging Technologies	
22	**Quantum Networking Risks**	**Quantum Networking Risks** Post-quantum cryptography, QKD (Quantum Key Distribution)	LO4: Trends & Emerging Technologies	
23	**Review**	**Project** Design and defend a secure enterprise network	LO4: Trends & Emerging Technologies	
24	**5G Security Challenges**	**5G Security Challenges** Network slicing risks, edge computing threats	LO4: Trends & Emerging Technologies	
25	**IoT Security**	**IoT Security** Zigbee/Wi-Fi 6 vulnerabilities, device hardening	LO4: Trends & Emerging Technologies	
26	**Network Hardening Lab**	**Network Hardening Lab** Configure NGFW, IDS, VPN on pfSense/OPNsense	LO5: Hands-On & Capstone	
27	**Incident Simulation**	**Incident Simulation** Respond to a ransomware attack on a mock network	LO5: Hands-On & Capstone	
28	**Research Paper/Presentation**	**Research Paper/Presentation** Analyze an emerging tech (e.g., SASE, ZTNA)	LO5: Hands-On & Capstone	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	