INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» eylül

Programme	**LEVEL 4 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 3 NETWORK SECURITY**		
Cohort Code:	L04NWS-U3		
Unit Level	Level 4		
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 module is designed to provide students with a thorough understanding of network security principles and practices. It aims to develop competence in identifying and mitigating network threats and vulnerabilities to prepare students for professional roles in network 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** • Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson. • Kurose, J. F., & Ross, K. W. (2020). Computer Networking: A Top-Down Approach. Pearson. • Easttom, C. (2018). Network Defense and Countermeasures: Principles and Practices. Pearson. • Doyle, J. (2016). Cisco Networking All-in-One For Dummies. Wiley.

Learning Outcome	Assessment Criteria
LO1: Understand the fundamentals of network security.	1.1 : Define key concepts and principles of network security. 1.2 : Explain the types of network threats and vulnerabilities. 1.3 : Describe the development and trends in network security.
LO2: Implement security measures to protect network infrastructure.	2.1 : Identify and apply network security controls and protocols. 2.2 : Configure and manage security devices such as firewalls and intrusion detection systems (IDS). 2.3 Evaluate the effectiveness of security measures in protecting network infrastructure.
LO3: Conduct network security assessments.	3.1 Perform network security assessments to identify potential vulnerabilities. 3.2 Analyze network traffic to detect and respond to security incidents 3.3 Develop a report detailing findings and recommendations from network security assessments
LO4: Develop and implement network security policies.	4.1 Design network security policies and procedures. 4.2 Implement network security policies in an organizational setting. 4.3 Evaluate the effectiveness of network security policies and update them as

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Network Security**	**Introduction to Network Security** CIA Triad (Confidentiality, Integrity, Availability) in networks	LO1: Fundamentals of Network Security	
2	**Network Security Terminologies**	**Network Security Terminologies** Threats, vulnerabilities, exploits, attack vectors	LO1: Fundamentals of Network Security	
3	**Common Network Threats**	**Common Network Threats** DDoS, MITM, packet sniffing, IP spoofing	LO1: Fundamentals of Network Security	
4	**Network Vulnerabilities**	**Network Vulnerabilities** Unpatched systems, misconfigured devices, weak encryption	LO1: Fundamentals of Network Security	
5	**Evolution of Network Security**	**Evolution of Network Security** From firewalls to Zero Trust Architecture (ZTA)	LO1: Fundamentals of Network Security	
6	**Network Security Controls**	**Network Security Controls** ACLs (Access Control Lists), VLANs, segmentation	LO2: Network Security Implementation	
7	**Cryptographic Protocols**	**Cryptographic Protocols** SSL/TLS, IPsec, VPNs (OpenVPN, WireGuard)	LO2: Network Security Implementation	
8	Review	- Review of LO1 topics - Practice questions and mock assessment	LO1 LO2	

9	**Firewall Configuration**	**Firewall Configuration** Stateful vs. stateless, WAFs (Web Application Firewalls)	LO2: Network Security Implementation	
10	**Intrusion Detection/Prevention Systems (IDS/IPS)**	**Intrusion Detection/Prevention Systems (IDS/IPS)** Snort, Suricata, rule-based detection	LO2: Network Security Implementation	
11	**Endpoint Security**	**Endpoint Security** NAC (Network Access Control), EDR (Endpoint Detection and Response)	LO2: Network Security Implementation	
12	**Vulnerability Scanning**	**Vulnerability Scanning** Tools: Nessus, OpenVAS, Nmap scripts	LO3: Network Assessments & Monitoring	
13	**Penetration Testing**	**Penetration Testing** Ethical hacking phases (recon, scanning, exploitation)	LO3: Network Assessments & Monitoring	
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	**Network Traffic Analysis**	**Network Traffic Analysis** Wireshark, tcpdump for anomaly detection	LO3: Network Assessments & Monitoring	

18	**SIEM (Security Information & Event Management)**	**SIEM (Security Information & Event Management)** Splunk, ELK Stack, Microsoft Sentinel	LO3: Network Assessments & Monitoring	
19	**Incident Response**	**Incident Response** NIST SP 800-61 framework, forensic triage	LO3: Network Assessments & Monitoring	
20	**Security Policy Design**	**Security Policy Design** Components: Acceptable use, BYOD, remote access	LO4: Security Policies & Governance	
21	**Access Control Models**	**Access Control Models** RBAC (Role-Based Access Control), ABAC (Attribute-Based)	LO4: Security Policies & Governance	
22	**Disaster Recovery & BCP**	**Disaster Recovery & BCP** RTO (Recovery Time Objective), RPO (Recovery Point Objective)	LO4: Security Policies & Governance	
23	Review	**Project** Secure a mock enterprise network (design + report)		
24	**Compliance Standards**	**Compliance Standards** ISO 27001, NIST CSF, PCI-DSS	LO4: Security Policies & Governance	
25	**Policy Auditing & Updates**	**Policy Auditing & Updates** Continuous monitoring, version control	LO4: Security Policies & Governance	
26	**Firewall & IDS Lab**	**Firewall & IDS Lab** Configure pfSense/Sophos, create custom Snort rules	LO5: Hands-On Labs & Case Studies	
27	**VPN Setup**	**VPN Setup** Site-to-site and remote-access VPN implementation	LO5: Hands-On Labs & Case Studies	

28	**Attack Simulation**	**Attack Simulation** MITM with Ettercap, DDoS mitigation	LO5: Hands-On Labs & Case Studies	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	