INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» eiyul

Programme	**LEVEL 4 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 4 OPERATING SYSTEM SECURITY**		
Cohort Code:	L04OSS-U4		
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 aims to provide students with a comprehensive understanding of operating system security principles and practices. It prepares students to secure various operating systems by implementing appropriate security measures and addressing potential vulnerabilities.
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** • "Security Strategies in Windows Platforms and Applications" by Michael G. Solomon and K. Rudolph - This book provides in-depth coverage of security issues and solutions specific to Windows operating systems. • "The Art of Computer Virus Research and Defense" by Peter Szor - A comprehensive guide to understanding, detecting, and defending against computer viruses and malware. • "Linux Security Cookbook" by Daniel J. Barrett, Richard E. Silverman, and Robert • G. Byrnes - Offers practical advice and solutions for securing Linux operating systems. • "Hacking Exposed Windows: Microsoft Windows Security Secrets and Solutions" by Joel Scambray and Stuart McClure - Focuses on the security vulnerabilities of Windows operating systems and provides strategies for defending against attacks. • "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" by Bill Blunden - Discusses advanced rootkit techniques and countermeasures for protecting operating systems. • "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown - Covers broad principles of computer security, including operating system security.

Learning Outcome	Assessment Criteria
LO1. Understand the fundamentals of operating system security.	1.1. Explain the core concepts and principles of operating system security. 1.2. Identify common security threats and vulnerabilities specific to operating systems. 1.3. Describe the evolution of operating system security and current trends
LO2. Implement security measures to protect operating systems.	2.1. Apply security configurations to different operating systems. 2.2. Manage and update security patches and service packs effectively. 2.3. Use security tools and software to enhance operating system security.
LO3. Conduct security assessments for operating systems.	3.1: Perform security audits and vulnerability assessments on operating systems. 3.2: Analyze audit logs to identify and respond to security incidents. 3.3: Develop reports detailing the findings and recommendations from security assessments.
LO4. Develop and implement operating system security policies.	4.1: Design comprehensive security policies for operating systems. 4.2: Implement operating system security policies within an organization. 4.3: Evaluate and update security policies regularly to address emerging threats.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to OS Security**	**Introduction to OS Security** CIA Triad (Confidentiality, Integrity, Availability) in OS context	LO1: Fundamentals of OS Security	
2	**OS Security Architectures**	**OS Security Architectures** Kernel vs. user space, reference monitor, security rings	LO1: Fundamentals of OS Security	
3	**Common OS Threats**	**Common OS Threats** Privilege escalation, rootkits, buffer overflows	LO1: Fundamentals of OS Security	
4	**Vulnerabilities in OS**	**Vulnerabilities in OS** Zero-day exploits, misconfigurations, unpatched systems	LO1: Fundamentals of OS Security	
5	**Evolution of OS Security**	**Evolution of OS Security** From UNIX to modern systems (Windows, Linux, macOS)	LO1: Fundamentals of OS Security	
6	**Security Configurations**	**Security Configurations** Windows Group Policy, Linux SELinux/AppArmor	LO2: OS Hardening & Protection	
7	**Patch Management**	**Patch Management** WSUS (Windows), apt/yum (Linux), automated patching	LO2: OS Hardening & Protection	
8	Review	- Review of LO1 topics - Practice questions and mock assessment	LO1 LO2	
9	**Endpoint Protection**	**Endpoint Protection** Antivirus, EDR (Endpoint Detection and Response)	LO2: OS Hardening & Protection	
10	**Authentication & Access Control**	**Authentication & Access Control** Multi-factor authentication (MFA), RBAC (Role-Based Access Control)	LO2: OS Hardening & Protection	

11	**Disk & File Encryption**	**Disk & File Encryption** BitLocker (Windows), LUKS (Linux), FileVault (macOS)	LO2: OS Hardening & Protection	
12	**OS Auditing Tools**	**OS Auditing Tools** Windows Event Viewer, Linux auditd, SIEM integration	LO3: Security Assessments & Monitoring	
13	**Vulnerability Scanning**	**Vulnerability Scanning** Nessus, OpenVAS, Lynis (Linux)	LO3: Security 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	**Log Analysis**	**Log Analysis** Splunk, ELK Stack, anomaly detection	LO3: Security Assessments & Monitoring	
18	**Incident Response for OS**	**Incident Response for OS** Forensic tools (FTK, Autopsy), memory analysis (Volatility)	LO3: Security Assessments & Monitoring	
19	**Penetration Testing**	**Penetration Testing** Metasploit, Mimikatz for privilege escalation	LO3: Security Assessments & Monitoring	
20	**OS Security Policy Design**	**OS Security Policy Design** Password policies, least privilege, remote access rules	LO4: Security Policies & Governance	
21	**Compliance Standards**	**Compliance Standards** CIS Benchmarks, NIST SP 800-53,	LO4: Security Policies & Governance	

		ISO 27001		
22	**Disaster Recovery**	**Disaster Recovery** System backups, bare-metal recovery, snapshots	LO4: Security Policies & Governance	
23	Review	**Project** Secure a multi-OS environment (design + report)	LO4: Security Policies & Governance	
24	**Policy Implementation**	**Policy Implementation** GPO (Windows), Puppet/Ansible (Linux)	LO4: Security Policies & Governance	
25	**Continuous Monitoring**	**Continuous Monitoring** SIEM alerts, automated compliance checks	LO4: Security Policies & Governance	
26	**Windows Hardening Lab**	**Windows Hardening Lab** Configure GPO, disable unnecessary services	LO5: Hands-On Labs & Case Studies	
27	**Linux Security Lab**	**Linux Security Lab** Set up SELinux, firewall (iptables/nftables)	LO5: Hands-On Labs & Case Studies	
28	**Incident Simulation**	**Incident Simulation** Detect and respond to a ransomware attack	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	