THE INTERNATIONAL QUALIFICATIONS AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» 09

Programme	International Foundation Year Diploma in Information Technology (RQF)		
Unit Number/ Unit Title	**Unit 3 Networking and Security**		
Cohort Code:	L03NCS-U3		
Unit Level	Level 3		
Total GLH	Total qualification time 120/ Total Guided learning hours 48/ Self-guided learning hours 72		
Credits	12 CATS/ 6 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This unit aims to provide students with an understanding of networking concepts and principles, as well as fundamental knowledge in cybersecurity. Companies of all scales and sizes want to have proper strategies and mitigation processes to secure their networks. Although there are no networks that are completely secured from cyber threats, an efficient and reliable network security system can ensure that essential security is maintained. The Network Security Training course from Infosectrain is designed to help you build a basic understanding of Networks and their various components. The course extensively covers a wide range of concepts along with tools used to secure networks. This training program will help you identify and mitigate various types of Network Security threats and attacks that plague Network security systems like Sniffing, DoS & DDoS attacks, Fraggle and Smurf attacks, DNS poisoning, etc.

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** • "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross • "Network Security Essentials: Applications and Standards" by William Stallings

Learning Outcome	Assessment Criteria
LO1. Understand the principles and concepts of computer networking.	1.1 Define what a computer network is and its purpose. 1.2 Describe different types of networks (LAN, WAN, MAN). 1.3 Explain the basic components of a network (router, switch, modem).
LO2. Demonstrate knowledge of network protocols and technologies	2.1 Identify and explain common network protocols (TCP/IP, UDP, HTTP) 2.2 Describe network topologies and their advantages/disadvantages. 2.3 Demonstrate understanding of network security measures (firewalls, encryption).
LO3. Analyze cybersecurity threats and measures.	3.1 Identify common cybersecurity threats (malware, phishing, DDoS). 3.2 Evaluate strategies for securing networked systems and data. 3.3 Discuss ethical and legal considerations in cybersecurity.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1.	**Introduction to Networks**	**Introduction to Networks** – Definition, purpose, and evolution of computer networks	**LO1: Networking Fundamentals**	
2.	**Network Types**	**Network Types** – LAN, WAN, MAN, PAN, WLAN (real-world examples)	**LO1: Networking Fundamentals**	
3.	**Network Components**	**Network Components** – Routers, switches, modems, APs, NICs (hardware demo)	**LO1: Networking Fundamentals**	
4.	**OSI & TCP/IP Models**	**OSI & TCP/IP Models** – Layer-by-layer breakdown with analogies	**LO1: Networking Fundamentals**	
5.	**Transmission Media**	**Transmission Media** – UTP, fiber optic, wireless (pros/cons)	**LO1: Networking Fundamentals**	
6.	**IP Addressing Basics**	**IP Addressing Basics** – IPv4 vs. IPv6, subnetting introduction	**LO1: Networking Fundamentals**	
7.	**Network Architectures**	**Network Architectures** – Client-server vs. peer-to-peer (case studies)	**LO1: Networking Fundamentals**	
8.	**TCP/IP Suite**	**TCP/IP Suite** – TCP vs. UDP, ports, and packet structure	**LO2: Protocols & Technologies**	
9.	**Application Layer Protocols**	**Application Layer Protocols** – HTTP/HTTPS, FTP, DNS, SMTP	**LO2: Protocols & Technologies**	
10.	**Network Topologies**	**Network Topologies** – Star, bus, ring, mesh (simulations with Cisco Packet Tracer)	**LO2: Protocols & Technologies**	
11.	**Wireless Technologies**	**Wireless Technologies** – Wi-Fi standards (802.11a/b/g/n/ac/ax), Bluetooth, NFC	**LO2: Protocols & Technologies**	
12.	**Routing & Switching**	**Routing & Switching** – Static vs. dynamic routing (RIP, OSPF)	**LO2: Protocols & Technologies**	
13.	**Firewalls & IDS/IPS**	**Firewalls & IDS/IPS** – Packet filtering, stateful inspection	**LO2: Protocols & Technologies**	
14.	**Encryption Basics**	**Encryption Basics** – Symmetric (AES) vs. asymmetric (RSA), SSL/TLS	**LO2: Protocols & Technologies**	
15.	Midterm	Midterm		

16.	**Threat Landscape**	**Threat Landscape** – Malware (viruses, worms, ransomware), zero-day exploits	**LO3: Cybersecurity Essentials**	
17.	**Social Engineering**	**Social Engineering** – Phishing, vishing, baiting (demo with mock emails)	**LO3: Cybersecurity Essentials**	
18.	**DDoS Attacks**	**DDoS Attacks** – Botnets, amplification attacks (Wireshark analysis)	**LO3: Cybersecurity Essentials**	
19.	**Authentication Methods**	**Authentication Methods** – Passwords, MFA, biometrics, OAuth	**LO3: Cybersecurity Essentials**	
20.	**Access Control Models**	**Access Control Models** – RBAC, DAC, MAC	**LO3: Cybersecurity Essentials**	
21.	**Vulnerability Assessment**	**Vulnerability Assessment** – Introduction to Nessus/OpenVAS	**LO3: Cybersecurity Essentials**	
22.	**Ethical Hacking Basics**	**Ethical Hacking Basics** – Pen testing phases (recon, scanning, exploitation)	**LO3: Cybersecurity Essentials**	
23.	**Legal Frameworks**	**Legal Frameworks** – GDPR, HIPAA, Computer Misuse Act	LO3: Cybersecurity Essentials	
24.	**Lab 1: Build a LAN**	**Lab 1: Build a LAN** – Physical cabling + IP configuration	**Hands-On Labs & Projects**	
25.	**Lab 2: Wireshark Traffic Analysis**	**Lab 2: Wireshark Traffic Analysis** – Filtering HTTP vs. DNS packets	**Hands-On Labs & Projects**	
26.	**Lab 3: Configure a Firewall**	**Lab 3: Configure a Firewall** – Windows Defender/iptables rules	**Hands-On Labs & Projects**	
27.	**Lab 4: Password Cracking**	**Lab 4: Password Cracking** – Using John the Ripper (ethical context)	**Hands-On Labs & Projects**	
28.	**Lab 5: VPN Setup**	**Lab 5: VPN Setup** – OpenVPN/WireGuard configuration	**Hands-On Labs & Projects**	
29.	**Lab 6: Phishing Simulation**	**Lab 6: Phishing Simulation** – Creating awareness campaigns	**Hands-On Labs & Projects**	
30.	**Emerging Trends**	**Emerging Trends** – SDN, IoT security challenges	**Extended Topics & Assessments**	
31.	**Incident Response**	**Incident Response** – Steps in a data breach scenario	**Extended Topics & Assessments**	
32.	**Cryptography Workshop**	**Cryptography Workshop** – Caesar cipher to PGP demo	**Extended Topics & Assessments**	

33.	**Debate: Privacy vs. Security**	**Debate: Privacy vs. Security** – Government surveillance cases	**Extended Topics & Assessments**	
34.	**Case Study Analysis**	**Case Study Analysis** – SolarWinds, Equifax breaches	**Extended Topics & Assessments**	
35.	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
36.	Final Exam		LO1, LO2, LO3, LO4	