SECU: Enterprise Network Security

Module Title:	Enterprise Network Security
Language of Instruction:	English

Credits:	5

NFQ Level:	8

Module Delivered In	1 programme(s)

Teaching & Learning Strategies:	A combination of traditional lectures and laboratory sessions will be employed. The laboratory sessions will allow for regular formative assessment and feedback.

Module Aim:	To provide the learners with the knowledge and skills to design, configure, maintain and troubleshoot a secure network.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Appraise threats and vulnerabilities to network and information security.
LO2	Evaluate wired and wireless LAN vulnerabilities and justify mitigation techniques to reduce the attack surface.
LO3	Plan, install, troubleshoot and monitor security infrastructure and peripheral equipment

Pre-requisite learning		
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*		
8917	NETW	Networking III
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module.*		
No incompatible modules listed		
Co-requisite Modules		
No Co-requisite modules listed		
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.*		
No requirements listed		

Module Content & Assessment

Indicative Content
Wired and Wireless LAN Security: Endpoint vulnerabilities and protective measures, Layer 2 vulnerabilities and security measures, Switch security features (e.g. Port Stealing, Switch flooding, storm control), rogue Access Points and devices, man-in-the-middle attacks
Authentication, Authorisation and Accounting (AAA): Local and server based authentication, server based authorisation and accounting (e.g. RADIUS and TACACS+). Network Access Control (NAC), IEEE 802.1X
Firewalls: Review ACLs, Configure firewalls, Implement and evaluate stateless, stateful, circuit-level, application and next gen firewalls (zone-based policy firewalls, IP tables), Context-based Access Control (CBAC), DMZ
IDS & IPS IDS v IPS, Types of IPSs (e.g. Pattern-based detection, Anomaly-based detection, Policy-based detection, Honey pot-based detection), IPS Evasion Techniques (e.g. Evader: Encryption and Tunnelling, Timing Attacks, Resource Exhaustion, Traffic Fragmentation, Protocol-level Misinterpretation), Anti-evasion countermeasures
Log File and Traffic Analysis: Read, translate and analyse logs generated for event; Traffic monitoring and analysis, Tools (e.g. Kibana, Sguil & Wireshark)

Assessment Breakdown	%
Continuous Assessment	50.00%
Project	40.00%
Practical	10.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Examination	.	1,2,3	20.00	Week 6
Examination	.	1,2,3	30.00	Week 9

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	.	1,2,3	40.00	Week 12

Practical

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	Weekly practical/laboratory work is designed to allow students to demonstrate the achievement of all the learning outcomes.	1,2,3	10.00	n/a

No End of Module Formal Examination

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time

Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	2.00
Laboratory	12 Weeks per Stage	2.00
Estimated Learner Hours	15 Weeks per Stage	5.13
	Total Hours	125.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	7	Mandatory