SYST: Systems Infrastructure and Security

Module Title:	Systems Infrastructure and Security
Language of Instruction:	English

Credits:	5

NFQ Level:	6

Module Delivered In	5 programme(s)

Teaching & Learning Strategies:	Learning is divided into lecture and practical sessions over one semester. The practical sessions will provide students with hands on experience in installing, configuring and securing a computer system infrastructure. It will also provide the opportunity to implement and reinforce material presented in lectures, to learn by doing.

Module Aim:	To provide learners with the necessary skills to build and secure a computer system infrastructure.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Demonstrate theoretical and practical knowledge of securing a system infrastructure.
LO2	Implement automated protection and monitoring software across a system infrastructure.
LO3	Describe industry standard frameworks available to ensure system security.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*
No recommendations listed
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
Computer Security Review of CIA model, OS updates and package management, verifying checksums on downloaded packages.
Securing Systems Securing against common vulnerabilities (e.g. XSS, DDoS, DNS Poisoning). Security keys and key management (e.g. SSH and PGP). Encryption and encryption tools e.g. VeraCrypt.
System Monitoring Setup and configuration of automated monitoring software such as Nagios and Zabbix to monitor system processes, usage of system resources, and file systems. Examine Nikto for Web Servers.
Security Tools Configuring firewalls, implementing honeypots and examining SIEM and IDS tools such as Snort, security scanning tools such as Nessus.
Mitre Attack Framework Overall analysis and evaluation of the Mitre Attack Framework and implementation of sections where appropriate.

Assessment Breakdown	%
Continuous Assessment	10.00%
Project	50.00%
End of Module Formal Examination	40.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Short Answer Questions	Diagnostic assessment	1	10.00	Week 5

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	System security project	1,2	50.00	Week 10

No Practical

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	End of semester exam	1,3	40.00	End-of-Semester

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

SYST: Systems Infrastructure and Security

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	1.00
Laboratory	12 Weeks per Stage	3.00
Independent Learning	15 Weeks per Stage	5.13
	Total Hours	125.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KWCCD_B	Bachelor of Science (Honours) in Creative Computing and Digital Innovation	4	Mandatory
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	4	Mandatory
CW_KCCIT_B	Bachelor of Science (Honours) in Information Technology Management	4	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	4	Mandatory
CW_KCCSY_D	Bachelor of Science in Information Technology Management	4	Mandatory