

Module Title:	Secure Systems Administration
Language of Instruction:	English
Credits:	10
NFQ Level:	7
Module Delivered In	2 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 configuring, managing and administering a secure computer domain. It will also provide the opportunity to implement and reinforce material presented in the lectures.
Module Aim:	To provide learners with the theoretical knowledge and practical skills required for deploying and administering a secure computer domain.
Learning Outcomes	
<i>On successful completion of this module the learner should be able to:</i>	
LO1	Explain best practice as related to managing and administering systems and services securely.
LO2	Compare and contrast client/server and peer to peer system architecture.
LO3	Integrate directory services, DNS, DHCP and a web server to provide domain services as part of a computer system.
LO4	Create and implement robust computer security policies manually and via scripting.
LO5	Interpret the role of regulation such as GDPR, as it applies to system administration.
Pre-requisite learning	
Module Recommendations	
<i>This is prior learning (or a practical skill) that is recommended before enrolment in this module.</i>	
No recommendations listed	
Incompatible Modules	
<i>These are modules which have learning outcomes that are too similar to the learning outcomes of this module.</i>	
No incompatible modules listed	
Co-requisite Modules	
No Co-requisite modules listed	
Requirements	
<i>This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.</i>	
No requirements listed	

Module Content & Assessment

Indicative Content

Server Systems

Analysing operating systems software capable of providing an array of secure services to clients. Investigating the requirements of the software and the limitations of the operating system. Evolution of server software releases and determining the version to implement.

Security Policy

Security policy standards and governance. Information security, network security, non-technical security. Policy types and examples. Contingency planning and security policy enforcement.

Directory Services

Directory services model, functionality and structure. Example implementations of LDAP and tree designs (root, branches and leaf objects). Objects, schema and organisational units.

DNS

Role of DNS and decentralised structure. Root servers and zones. DNS namespace forward and reverse lookups. Authoritative vs. Non-authoritative. Recursive vs. Non-recursive. Security issues with DNS.

DHCP

DHCP role in a network, static vs dynamic addressing. DHCP operating and interaction. Configuration of service and creation of scopes. Security issues with DHCP.

Web Server

Implementation of HTTP and HTTPS. URI, URL and URNs. HTML and GET/POST requests. HTTP status codes. Vulnerabilities of HTTP.

Securing Systems

Securing servers and systems, server OS and application hardening. Examining and protecting against common vulnerabilities on a domain.

Scripting

Automation and configuration via a command line interpreter/scripting environment. Pipelines and filtering. Testing and securing systems using shell tools and utilities.

Legal Regulations

Examination, analysis and interpretation of relevant legislation such as GDPR, as it applies to the role of a systems administrator.

Assessment Breakdown	%
Continuous Assessment	20.00%
Project	40.00%
End of Module Formal Examination	40.00%

Continuous Assessment				
Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Short Answer Questions	Diagnostic Assessment	1,2	20.00	Week 6

Project				
Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Project	Systems Project	3,4	40.00	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	1,5	40.00	End-of-Semester

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

Module Workload

Workload: Full Time		
<i>Workload Type</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Lecture	12 Weeks per Stage	1.00
Laboratory	12 Weeks per Stage	4.00
Tutorial	12 Weeks per Stage	1.00
Independent Learning	15 Weeks per Stage	11.87
Total Hours		250.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCIT_B	Bachelor of Science (Honours) in Information Technology Management	5	Mandatory
CW_KCCSY_D	Bachelor of Science in Information Technology Management	5	Mandatory