COAP: Scripting for Cybersecurity

Module Title:	Scripting for Cybersecurity
Language of Instruction:	English

Credits:	10

NFQ Level:	6

Module Delivered In	2 programme(s)

Teaching & Learning Strategies:	As well as traditional lectures learners will undertake various laboratory exercises. Learners will be expected to actively participate in class and work throughout each scheduled lab session to accomplish assigned tasks.

Module Aim:	To provide learners with a theoretical knowledge and the practical skills to automate cybersecurity tasks such as network traffic manipulation and Web application and network infrastructure fingerprinting.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Applying programming concepts to automate cybersecurity tasks.
LO2	Utilise programming language and libraries for network traffic manipulation
LO3	Utilise programming language features and libraries for Web application and network infrastructure fingerprinting and reconnaissance

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

COAP: Scripting for Cybersecurity

Module Content & Assessment

Indicative Content
Scripting Essentials Environment processing, Argument processing, Piping, teeing, globbing, and process control, Interacting with daemon processes.
Interacting with running OS processes and tasks: Sending input data to running processes, Capturing output from running processes
Analysis of output data: Understanding scripting data structures, I/O: files, streams, and databases.
Applying DRY principles to scripting: functions, modules, and packages, Log processing, fingerprinting and reconnaissance.

Assessment Breakdown	%
Project	100.00%

No Continuous Assessment

Project

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	Project on content up to week 5	1,2	30.00	Week 5
Project	Project on content up to week 8	1,2,3	30.00	Week 8
Project	Project on content up to week 12	1,2,3	40.00	Week 13

No Practical

No End of Module Formal Examination

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

COAP: Scripting for Cybersecurity

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	12 Weeks per Stage	2.00
Laboratories	12 Weeks per Stage	4.00
Independent Learning Time	15 Weeks per Stage	11.87
	Total Hours	250.00

Module Delivered In

Programme Code	Programme	Semester	Delivery
CW_KCCYB_B	Bachelor of Science (Honours) in Cyber Crime and IT Security	3	Mandatory
CW_KCCYB_D	Bachelor of Science in Cybercrime and IT Security	3	Mandatory