Title:	Windows Security APPROVED
Long Title:	Windows Security

Module Code:	COMP7045	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Intermediate
Field of Study:	Computer Science
Valid From:	Semester 1 - 2019/20 (September 2019)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	VINCENT RYAN
Module Description:	In this module students will learn about Operating System's and its registries in a Windows environment and its application in security in particular. In addition, the student will learn about typical filesystems such as NTFS and how artefacts can be found that might be useful in a forensics investigation. It will also consider how an enterprise wide system such as Active Directory (AD) works and how Group Policy Objects (GPO) can be used. Finally, it will look at authentication in an enterprise system such as Kerberos.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Apply powershell scripting to automate security and other related tasks.
LO2	Locate and evaluate forensic artefacts in a Windows operating system.
LO3	Illustrate how authentication works in an enterprise wide system such as Active Directory
LO4	Carry out tasks on individual and on groups of hosts in an enterprise wide system.
LO5	Appraise the main keys in a systems such as the Windows registry.

Pre-requisite learning
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
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. You may not enrol on this module if you have not acquired the learning specified in this section.*
No requirements listed
Co-requisites
No Co Requisites listed

Module Content & Assessment

Indicative Content
PowerShell and WMIC Scripting with PowerShell; Adding and removing roles; getting a remote inventory; dealing with service failure; setting password policies; getting an app inventory, Use of WMIC.
FileSystem Study How a filesystem such as FAT and/or NTFS works. Boot Sector, MBR, MFT, logfile, bitmap, boot, permissions, volume shadow copy.
Forensics Introduction Allocated and unallocated space, slack space, file carving, imaging a drive, artefact location, timestamps.
Remote Administration Performing tasks on individual and on groups of hosts in an enterprise wide system, including tasks which help secure users and computers/servers in a domain. Secure user authentication.
Windows Internals The Registry, local accounts, Security applications such as AppLocker, backup and restore, use of tools such as regshot and procmon. Keys and values.

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Short Answer Questions	Examine the student's knowledge of some of the theoretical aspects of the module.	1,3,4	25.0	Week 5
Practical/Skills Evaluation	Students will be assessed on a number of assigned tasks. This assessment may be focused on Powershell scripting tasks where they will be asked to perform various tasks on the system.	1,4	20.0	Week 7
Short Answer Questions	Examine the student's knowledge of the main theoretical aspects of the module.	2,3,5	30.0	Week 11
Practical/Skills Evaluation	Lab based examination where students will be assessed on a number of assigned tasks. This assessment will focus mainly on forensics and remote administration.	2,4,5	25.0	Week 12

No End of Module Formal Examination

Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
Directed Learning	Directed learning.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Directed Learning	Directed Learning.	3.0	Every Week	3.00
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

- **Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich 2017, *Windows Internals, Part 1: System architecture, processes, threads, memory management, and more*, 7 Ed., Microsoft Press [ISBN: 9780735684188]**

Supplementary Book Resources

- **William Stanek 2015, *Windows Group Policy: The Personal Trainer for Windows Server 2012 and Windows Server 2012*, CreateSpace Independent Publishing Platform [ISBN: 9781512391633]**
- **Philip Polstra 2016, *Windows Forensics with Python Scripting*, CreateSpace [ISBN: 9781535312431]**
- **Harlan Carvey 2016, *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry*, 2 Ed., Syngress [ISBN: 9780128032916]**
- **Ed Wilson 2015, *Windows PowerShell Step by Step*, Microsoft Press [ISBN: 9780735675117]**

This module does not have any article/paper resources

Other Resources

- **website: *Scripting Guy Blog***
  https://blogs.technet.microsoft.com/heys criptingguy/
- **website: *Windows Powershell Blog***
  https://blogs.msdn.microsoft.com/powersh ell/
- **website: *SANS Digital Forensics and Incident Response Blog***
  https://digital-forensics.sans.org/blog

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KITMN_8	Bachelor of Science (Honours) in IT Management	4	Mandatory
CR_KITSP_7	Bachelor of Science in Information Technology	4	Mandatory