COMP C7017: Applied Security

Module Details

Module Code:	COMP C7017
Full Title:	Applied Security APPROVED
Valid From:	Semester 1 - 2019/20 (June 2019)
Language of Instruction:	English
Duration:	1 Semester
Credits:	5
Module Owner::	Frances Byrne
Departments:	Unknown
Module Description:	Students completing this module will have a thorough understanding of threats to the security of a computer system including end devices and network components. The student should be able to identify and configure appropriate technologies to mitigate against such threats.

Module Learning Outcome	
On successful completion of this module the learner will be able to:	
#	**Module Learning Outcome Description**
MLO1	Identify modern security threats.
MLO2	Explain the basic principles of cryptography.
MLO3	Apply countermeasures to mitigate specific attacks against end devices and network devices.
MLO4	Deploy both network and end devices in a secure manner.
MLO5	Deploy firewalls, intrusion prevention systems, and VPNs.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named DkIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
No recommendations listed

Module Indicative Content
Security Basics Security principles, risk analysis, malware, common attacks, and defences.
Authentication, Authorisation and Accounting Verify user/host password policy.
Cryptography Symmetric and asymmetric, hash algorithms, digital signatures.
Security Hosts and Data Secure OS configuration, deployment and sandboxing. Hardware and firmware security.
Securing the Network ACL's, Firewalls, IPS, VPN, IPSec, Kerberos.

Module Assessment

Assessment Breakdown	%
Course Work	40.00%
Final Examination	60.00%

Module Special Regulation

Assessments

Full Time

Course Work

Assessment Type	Class Test	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	3,4,5
Duration in minutes	120		

Assessment Description
Practical Exam

Assessment Type	Continuous Assessment	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	Every Second Week	**Learning Outcome**	1,2,3,4,5
Duration in minutes	0		

Assessment Description
Written reports and case assignments. The student's ability to design, install and configure appropriate security mechanisms will be measured by practical test or by assignment. A case assignment will measure the student's ability to understand the overall management and deployment of a security subsystem.

No Project

No Practical

Final Examination

Assessment Type	Formal Exam	**% of Total Mark**	60
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	1,2
Duration in minutes	0		

Assessment Description
End-of-Semester Final Examination

Part Time

Course Work

Assessment Type	Class Test	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	3,4,5
Duration in minutes	120		

Assessment Description
Practical Exam

Assessment Type	Continuous Assessment	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	Every Second Week	**Learning Outcome**	1,2,3,4,5
Duration in minutes	0		

Assessment Description
Written reports and case assignments. The student's ability to design, install and configure appropriate security mechanisms will be measured by practical test or by assignment. A case assignment will measure the student's ability to understand the overall management and deployment of a security subsystem.

No Project

No Practical

Final Examination

Assessment Type	Formal Exam	**% of Total Mark**	60
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	1,2
Duration in minutes	0		

Assessment Description
End-of-Semester Final Examination

Reassessment Requirement

A repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

Reassessment Description
The case assignments and practical exam will be repeatable

Module Workload

Workload: Full Time

Workload Type	*Contact Type*	*Workload Description*	*Frequency*	*Average Weekly Learner Workload*	*Hours*
Lecture	Contact		Every Week	2.00	2
Practical	Contact		Every Week	2.00	2
Directed Reading	Non Contact	No Description	Every Week	2.00	2
Independent Study	Non Contact		Every Week	2.00	2
				Total Weekly Learner Workload	8.00
				Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Contact Type*	*Workload Description*	*Frequency*	*Average Weekly Learner Workload*	*Hours*
Lecture	Contact	No Description	Every Week	2.00	2
Practical	Contact	No Description	Every Week	2.00	2
Directed Reading	Non Contact	No Description	Every Week	2.00	2
Independent Study	Non Contact	No Description	Every Week	2.00	2
				Total Weekly Learner Workload	8.00
				Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

William Stallings. (2016), Network security essentials: applications and standards, 6th. 12, Pearson, [ISBN: 0133370437].

James Stewart. (2017), CompTIA Security+ Review Guide, 4th. 6, Sybex, p.672, [ISBN: 978-111941694].

Supplementary Book Resources

Gollman, Dieter. (2015), Introduction to Network Security: Theory and Practice, 2nd. 10, Wiley, p.440, [ISBN: 978-1-118-939].

This module does not have any article/paper resources

Other Resources

[website], SANS,
http://www.sans.org

[website], Cisco Inc.. Home Page,
http://www.cisco.com

[website], OWASAP,
https://owasp.org/