TECH07043
LAN Cybersecurity

Full Title	LAN Cybersecurity		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	07	**ECTS Credits**	10
Module Code	TECH07043	**Duration**	26 Weeks - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Mark Frain		
Co Authors	Pearse McDonnell, Seamus Dowling		

Module Description

This module will allow students to 'harden' an organisation's network infrastructure. It involves configuring network infrastructure to monitor and filter network traffic (ingress and egress) and raise alerts if outside established baselines. It examines protocols and services used to secure LAN/WAN (local area network/wide area network) access. Students will actively compromise networks and implement solutions to negate these compromises. The module also examines the methods used by malware to probe, compromise and propagate network infrastructure and the protocols and applications that can be used to mitigate against such attacks.

	Learning Outcomes ***On completion of this module the learner will/should be able to:***
1.	Analyse and identify modern security threats and develop security policies and Access Control Lists to prevent such attacks.
2.	Configure, test and deploy Intrusion Detection System and Intrusion Prevention System based Network Security solutions.
3.	Configure, test and troubleshoot various network security configurations such as Virtual Private Networks, Secure Sockets Layer, AAA and Firewalls.
4.	Security harden devices to prevent threats or attacks to networked systems.
5.	Identify security protocols required for security solutions in both Local and Wide Area Network environments.
6.	Analyze and deploy cryptographic algorithms to provide security solutions.

Indicative Syllabus

Switching

Introduction to Switching, Port Configuration; Configuring switch security- Port Security;

Introduction to VLANs, VLAN trunking Protocol.

Modern Security threats

Explain network threats, the basics of securing a network. Securing Network Devices Configure secure administrative access and router resiliency Secure IOS-based Routers using automated features

Firewalls /ACL's

Content-Based Firewall / Zone-based Firewall, ACL's.

Intrusion Detection Systems / Intrusion Prevention Systems

Use of IDS and IPS to develop network intrusion detection systems.

Authentication, Authorization, Accounting

Port security, broadcast storm control, secure admin access with AAA Local Authentication, implement AAA using TACACS and RADIUS

protocols and Authorization and Accounting, hardening of switches and routers using SDM.

Introduction to Cryptography

Introduction to types of encryption, hashes, and digital signatures, confidentiality, integrity, and authentication, data integrity and authentication, data confidentiality, authentication using a public key.

Symmetric Cryptography

DES, Triple-DES, AES, Attacks on cryptosystems.

Public-Key Cryptography

RSA, Elliptic Curve Cryptosystems, Diffie-Hellmann, Hash Function, Message Authentication Codes, Digital Signatures.

Email Security

PGP, S/MIME.

Practical Programme:

Configuring ACL's/Firewalls on Routers

Configuring VPN's on Routers

Configuring IPS/IDS on Routers

Configuring Certificate Authorities on Routers/Servers

Configuring Email Applications to use encryption.

Teaching and Learning Strategy

This module can be delivered via the traditional face-to-face delivery methodology or via a blended format (employing both online and offline methodologies.) or via an online format.

Traditional face-to face delivery format.

The module can be delivered in the traditional delivery method using lectures/tutorials (2 hours per week) and lab practical's (2 hours per week).

Blended delivery format.

The module can be delivered in the blended delivery method using a mixture of online delivery (approx.. 75%) and face-to-face engagement (approx. 25%).

Weekly online delivery will consist of, but not exclusive to, live lectures and webinars, pre-recordings, synchronous and asynchronous discussion forums and open educational resources (OER's), exercises and reading, accounting for approx. 2 hours per week.

Online delivery format.

The module can be delivered in an asynchronous online method.

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year. Marking criteria, deadlines and expectations will also be provided to the learner in advance. Constructive feedback will be provided in a timely manner and in an appropriate format.

Assessment Strategy

This module will comprise 100% continuous assessment. The learner will be assessed on their practical ability and theoretical knowledge of LAN Cyber Security.

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year. Marking criteria, deadlines and expectations will also be provided to the learner in advance. Constructive feedback will be provided in a timely manner and in an appropriate format.

Repeat Assessment Strategies

Repeat facilities will be accommodated in line with GMIT Code of Practice No. 3 Student Assessment: Marks & Standards procedures and in compliance with programme board decisions.

Decisions on nature of assessment will be linked to the need to achieve particular learning outcomes. They may be in the form of a written assessment, project or other relevant assessment. Individuals may be interviewed or asked to present their work in a formal student conference context to prove authenticity and ownership of work.

Indicative Coursework and Continuous Assessment:		**100 %**		
Form	***Title***	***Percent***	***Week (Indicative)***	***Learning Outcomes***
Assignment	Assignment 1	25 %	Week 6	1,4
In class exam	Practical Exam	25 %	Week 13	1,2,3,4
Assessment	Assignment 2	25 %	Week 19	1,2,3,5,6
In class exam	Practical Exam	25 %	Week 26	1,2,3,4,5,6

Full Time Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Weekly lecture and/or tutorial.	Flat Classroom	2	Weekly	2.00
Practical	Practical.	Computer Laboratory	2	Weekly	2.00

Online Learning Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online asynchronous delivery of content, via live & recorder webinars & interactions, video, audio and assignments.	Online	4	Weekly	4.00

Blended Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online asynchronous delivery of content, via live & recorder webinars & interactions, video, audio and assignments.	Not Specified	3.5	Weekly	3.50
Practical	Practical LAB	Computer Laboratory	2	Monthly	0.50

Required Reading Book List

Stallings, W., (2016). *Cryptography and Network Security*. Pearson.
ISBN 0134444280 ISBN-13 9780134444284

Literary Resources

Journal Resources

Online Resources

Programme Membership

GA_KNCSC_B07 202000 Bachelor of Science in Network Cybersecurity