TECH07047
Network Operating Systems Security

Full Title	Network Operating Systems Security		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	07	**ECTS Credits**	10
Module Code	TECH07047	**Duration**	Stage - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Pearse McDonnell		
Co Authors	Mark Frain, Seamus Dowling, Brian Mulhern		

Module Description

This module introduces the learner to modern operating systems concepts and technologies. Students will learn about the Linux and Windows operating systems. They will examine the tools and services that can be used to monitor network traffic and detect malicious activity. Using forensic analysis techniques students will learn to test the robustness of an organisation’s computing infrastructure and to take the necessary steps to protect it from attack.

☰	**Learning Outcomes** ***On completion of this module the learner will/should be able to:***
1.	Install and configure the Linux/Windows Operating Systems
2.	Identify, assess and mitigate operating system threats
3.	Utilise the UNIX and Powershell command sets to create shell scripts
4.	Utilise forensic tools to monitor and analyse the operating system for malicious activity
5.	Define operating system and security policies around reducing the threat surface

Indicative Syllabus

Virtualisation

Introduction to virtualisation

Managing operating systems in a virtualised environment (VirtualBox, Hyper-V or similar)

Linux

The Different Linux 'Flavours'

Install and use few versions of the Linux OS (Kali, Parrot, Ubuntu, Mint for example)

Desktop Environment, Workspace & System Manager

UNIX Command Line Interface:

Moving, copying, viewing and creating files and directories

Create / monitor / kill processes, Modify processor priorities

Installing and maintaining Software (Advanced Package Tool or similar)

Booting and shutting down the system

Users, groups and permissions

String manipulation - regular expressions

Streams, redirects and pipes

Scripting

Windows Powershell

UNIX Shell Scripts: Variables, command line arguments, if statements, while / for loops

Forensics

The concept of a honeypot

Case Study: Analysis of sample honeypot log files

Script writing to extract information from honeypot data – IP addresses, username/passwords, temporal patterns

Access Control Lists (ACLs) to log traffic

Abstraction

Staying anonymous with TOR browser

Anonsurf

Proxychains

OS Security and Performance

Malware, antivirus software

OS Updates, Server Firewall

Network analysers and scanners (Wireshark, NMAP or similar)

Intrusion detection tools (Snort or similar)

Password cracking tools

Encryption tools

System forensics - System Log and Event files, Hard disk analysis.

System performance features – load average, CPU time, idle time, RAM usage

Operating System Management

Windows Server administration – Active directory Domains, Sites, and Organisational Units

Group Policy Objects, User and Computer Security policies and settings

Integration of Linux systems in a Windows environment

OS Management using Powershell scripting and the WMI

OS Services

Web and email Servers – installation and testing

Cloud computing services – File Services, Clustering, and Migration

Backup and recovery software

Teaching and Learning Strategy

The teaching and learning for this module will be blended, employing both online and class/lab based methodologies. There will be online and offline lectures as well as a learning community online for learners to collaborate and work together. Learners will engage with peers and the lecturing team on campus on a monthly basis.

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

Assessment Strategy

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***
Assessment	Assignment 1	25 %	Week 8	1,3
In class exam	Assignment 2	25 %	Week 13	2,3
Assessment	Assignment 3	25 %	Week 18	3,4
In class exam	Assignment 4	25 %	Week 26	2,3,4,5

Full Time Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Lecture & Tutorial Session	Computer Laboratory	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***
Lecture	Lecture	Online	1.5	Weekly	1.50
Tutorial	Tutorial	Online	1	Weekly	1.00
Online Learning	Online Live Forum	Online	1	Weekly	1.00
Practical	Practical	Online	2	Monthly	0.50

Blended Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Lecture	Not Specified	1.5	Weekly	1.50
Tutorial	Tutorial	Not Specified	1	Weekly	1.00
Tutorial	Online Live Forum	Online	1	Weekly	1.00
Practical	Practical	Computer Laboratory	2	Monthly	0.50

Recommended Reading Book List

Blum, R., (2015). *Linux Command Line and Shell Scripting Bible*. 3rd Edition. Wiley.

Hein, T., (2017). *UNIX and Linux System Administration Handbook*. 5th Edition. Addison Wesley.

Krause, J., (2018). *Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016*. 1st Edition. Packt Publishing.

Holmes, L., (2012). *Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's Command Shell*. 3rd Edition. O'Reilly Media.

Literary Resources

Journal Resources

Online Resources

Programme Membership
GA_KNCSC_B07 202000 Bachelor of Science in Network Cybersecurity