Institiúid Teicneolaíochta Chorcaí
Cork Institute of Technology

COMP8022: Network Security

Title:	Network Security APPROVED
Long Title:	Network Security

Module Code:	COMP8022	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Advanced
Field of Study:	Computer Science
Valid From:	Semester 1 - 2017/18 (September 2017)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	Sean McSweeney
Module Description:	Network security is the activity associated with maintaining the confidentiality, integrity and availability of data traversing a network infrastructure. In this module, the learner will evaluate Internet security and encryption, firewalls, sniffing and packet crafting, Virtual Private Networks (VPNs), IPv6 security and Network Intrusion Detection and Response Systems (NIDRS).

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Identify and critically assess threats to network security, and data loss.
LO2	Install, configure, and evaluate firewalls in terms of their security effectiveness.
LO3	Configure and appraise Network Intrusion Detection and Response Systems (NIDRS).
LO4	Explain, install and configure Virtual Private Network (VPN) technology.
LO5	Evaluate the security of Internet Protocol version 6 (IPv6) Systems

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.*
Students should have a basic knowledge of Computer Networking, especially the main Networking protocols.
Co-requisites
No Co Requisites listed

Module Content & Assessment

Indicative Content
Internet Security & Encryption Encryption of static data, IPSec, AH, ESP, IKE, ISAKMP/Oakley, Tunnel mode, Transport mode, Virtual Private Networks (VPNs), SSH Tunneling, Cloud Security Issues.
Firewalls Packet Filters (ACLs), Stateful, Stateless, Bastion Host, Circuit Level, Application Gateway, SOCKS, DMZ, Host-Based Firewall, Egress Filtering, Network Address Translation (NAT), Multi-homing, IPTables/NetFilter, implementing NAT, Next-Generation Firewalls (NGFW).
Sniffers and Packet Crafting Libpcap, dSniff, Wireshark, tcpdump, Mitigation of Sniffer Attacks, ARP Cache Poisoning, Port Stealing, Switch flooding, DNS and IP Spoofing, Session Hijacking, Sequence Numbers, Ettercap, idle host scanning, Default TTLs, Countermeasures, Packet Crafting using eg hping, scapy.
Intrusion Detection & Prevention Types of IDSs, Deployment of IDS systems, inline, passive, taps, span ports, Network IDSs, Anomaly based Detection and Signature based Detection, Evasion Techniques, False Positives, NIDS implementation using e.g. Snort, Suricata. Data Loss Prevention.
IPv6 Security IPv6 Header, Extension Headers, IPv6 packet capture and interpretation, Fragmentation and IPv6, RA and ND attacks, IPv6 Attack tools, Firewalling IPv6, Crafting IPv6 packets (using scapy).

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	The learner will be assessed on a number of assigned tasks determining their capacity to apply the theoretical knowledge delivered during the lectures. This may include an assessment of network security threats, a detailed description of the deployment of defensive measures such as a firewall and IDS and their efficacy in defeating these threats.	1,2,3	30.0	Week 6
Practical/Skills Evaluation	The learner will be assessed on a number of assigned tasks that will assess their proficiency in the practical application and understanding of the topic area of this module. The learner may be required to utilize tools introduced in the laboratories.	4,5	30.0	Week 11
Short Answer Questions	An in class exam that will require the learner to demonstrate understanding of the theoretical content of the module.	1,2,3,4,5	40.0	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	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	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*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

- **Jeremy Faircloth 2016, *Penetration Tester's Open Source Toolkit*, Syngress [ISBN: 9780128021497]**

Supplementary Book Resources

- **Steve Suehring 2015, *Linux Firewalls: Enhancing Security with nftables and Beyond*, 4th Ed. Ed., Addison-Wesley Professional [ISBN: 9780134000022]**
- **Mark Rhodes-Ousley 2013, *Information Security: The Complete Reference*, 2nd Ed. Ed., McGraw-Hill Education [ISBN: 9780071784351]**
- **Eric Cole 2009, *Network Security Bible*, 2nd Ed. Ed., Wiley [ISBN: 9780470502495]**
- **Barrie Dempster, James Eaton-Lee 2007, *Configuring IPCop Firewalls: Closing Borders with Open Source*, Packet Publishing [ISBN: 9788184042368]**
- **John R. Vacca 2006, *Guide to Wireless Network Security*, Springer [ISBN: 9780387954257]**
- **Chuck Easttom 2005, *Network Defense and Countermeasures: Principles and Practices* [ISBN: 9780131711266]**

Supplementary Article/Paper Resources

- **Juniper Networks 2010, *VPN Decision Guide***
  https://www.juniper.net/us/en/local/pdf/whitepapers/2000232-en.pdf

Other Resources

- **Website: SANS Institute *Network Security Resources***
  https://www.sans.org/network-security/

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KITMN_8	Bachelor of Science (Honours) in IT Management	5	Mandatory
CR_KITSP_7	Bachelor of Science in Information Technology	5	Mandatory