Title	Secure Network Systems
Long Title	Secure Network Systems
Credits	5
NFQ Level	Advanced

Module Description:

Network security is the activity associated with the detection and prevention of unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. In this module, the learner will evaluate common cyber security threats and defense in depth techniques to defend against these threats. In particular, the module will provide the learner with the skills to apply and use various computer protection components such as Firewalls, VPN and Intrusion Detection and Response Systems (NIDRS) and security techniques such as zoning and encryption. At the end of this module the learner should have the ability to operate and interpret information collected from various network security equipment and network tools to implement a secure network architecture. This module was developed under the CyberSkills HCI Pillar 3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Evaluate Network Security Architecture and Defense in Depth (DiD) techniques to ensure the security of a network against a range of cyber security attacks.
LO2 Assess, configure and use a firewall to protect a network against a range of attacks.
LO3 Appraise, configure and use a Network Intrusion Detection and Response Systems (NIDRS) with the aim of protecting a network against various forms of attacks.
LO4 Explain, install and configure Virtual Private Network (VPN) technology.
LO5 Critically access the use of encryption to protect sensitive data and issues related to key management.

Indicative Content

Cyber threats, vulnerabilities and attack vectors
ENISA threat landscape i.e. malware, insider threats, web based attacks, botnets, information leakage, cyber espionage, identity theft, ransomware, data breaches, denial of service, spam, phishing, crypto jacking. Structure of threat landscape. Threat actors, agents and trends – attack vectors, misinformation, disinformation, fileless and memory attacks, multi staged and modular threats etc. Threat intelligence and sharing. CIA Triad. Vulnerabilities types for wired and wireless networks. Vulnerability assessment. Penetration testing. Vulnerability database i.e. CVE Details.

Network Security Architecture
Defense in Depth. Admin controls - policy and procedures. Technical Controls - network, hardware and software. Physical controls. Access measures. Workstation defense - anti spam. Data Protection. Perimeter Defense. Monitoring and Prevention.

Security Principles - Firewalls & Zoning
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). Skill in configuring and utilizing network protection components i.e. Firewall. Skill in configuring and utilizing computer protection components i.e.. Firewall. Skill in protecting a network against malware using a firewall.

Security Principles - Encryption & VPN
Encryption of static data. Symmetric encryption and Asymmetric. Trusted certificates. Key selection, lifecycle, management, key rotation techniques and concepts. Internet Key Exchange (IKE). ISAKMP/Oakley. IPSec, AH, Encapsulating Security Payload (ESP). Tunnel mode, Transport mode, Virtual Private Networks (VPNs), Remote access, SSH Tunnelling, Cloud Security Issues. Skill in configuring and utilizing network protection components i.e. VPN.

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. IDS and Malware detection. Skill in configuring and utilizing network protection components i.e. IDS. Skill in protecting a network against malware using a NIDS.

Network System Performance
Simple Network Management Protocol (SNMP). Network Traffic Monitoring tools. Wireshark. Nmap. Traceroute. Bandwidth Monitoring. Network Performance Indicators - CPUs, memory, temperature, throughput, latency. Ability to monitor measures or indicators of systems performance and availability. Ability to monitor traffic flows across the network. Skill in using network management tools to analyse network traffic patterns e.g. SNMP.

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 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. The learner will communicate their results using professional communication methods which may include the production of a laboratory book or portfolio of work as well written and oral presentations.	1,2	40.0	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. The learner will communicate their results using professional communication methods which may include the production of a laboratory book or portfolio of work as well written and oral presentations.	3,4,5	60.0	Sem End

No End of Module
Formal Exam

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent student 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*
Lecture	Lecture underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent student learning.	3.0	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

- **C. P. Gupta and K. K. Goyal 2020, Cybersecurity: A Self-Teaching Introduction, Mercury Learning & Information [ISBN: 9781683924982]**