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

Module Description:

This module is focused on the study of advanced system and network administration topics. Topics explored and implemented will include the setup and maintenance of many of the most popular network services including servers for DNS, LDAP and email (SMTP, POP3, IMAP). Special attention is paid to the concepts needed to implement these services securely and to the troubleshooting skills that will be necessary for real-world administration of these network services. At the end of this module learners should have the ability to operate, configure and secure various electronic communication systems, services and networks. 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	Assess how various network protocols are used to implement key network services.
LO2	Evaluate the security requirements and measures required to protect network services.
LO3	Implement and secure various network services found in electronic communications systems.
LO4	Review the main standards for deploying wireless communications in a network and best practices and configuration requirements to ensure that the wireless network is secure.

Indicative Content

Network Protocol - Domain Name System (DNS)

DNS history and theory, The domain name space, Delegation and Zones, Resolving names and reverse lookups, Configuring BIND named.conf, Configuring BIND zones, DNS hierarchies: subdomain delegation, Securing BIND DNS, BIND 9 Views, Restricting queries, Restricting zone transfers, DDNS and nsupdate, DNS-over-HTTPS (DoH).

Network Protocol - Lightweight Directory Access Protocol (LDAP)

LDAP Schema, Referencing LDAP entries, LDAP security, Implementing OpenLDAP server, Defining global parameters, Restricting access, Database configuration and indexing, Querying LDAP databases. SSL and TLS. Secure Server Configuration.

Network Protocol - Dynamic Host Configuration Protocol (DHCP)

IP address management. Components of DHCP. Benefits of DHCP. Security risks of DHCP. Network Security against DHCP attacks.

Electronic Comms System - Simple Mail Transfer Protocol (SMTP) SMTP theory, Implementing SMTP with Postfix, Postfix configuration, Postfix ESMTP AUTH and encryption, Email services: POP3 and IMAP4, Encrypting client access, Spam and virus filtering, Web mail client access.

Wireless Networks – Wifi

Wireless Local Area Networks (WLAN). 802.11 standard overview. Access Control security using Service Set Identifiers (SSID). MAC address filtering. Stream Ciphers. Wireless Encryption Protocol (WEP). Eavesdropping. Redundancy Checking (CRC-32). Denial of Service (DoS). Extensible Authentication Protocol (EAP). Temporal Key Integrity Protocol (TKIP). AES. Counter Mode CBC-MAC Protocol(CCMP).

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Short Answer Questions	A series of short answer question are asked to evaluate the student's capacity to assess how various network protocols are used to implement key network services and evaluate the security requirements and measures required to protect network services.	1,2	40.0	Week 8
Project	In this project students will implement and secure various electronic communications systems in a network and review the main standards for deploying wireless communications in a network and best practices and configuration requirements to ensure that the wireless network is secure. The learner will document the details of their project in a written report to a professional standard.	3,4	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 Leaner Workload*
Lecture	Lecture underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	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 Leaner Workload*
Lecture	Lecture underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	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

- Chris Sanders, Jason Smith 2013, Applied Network Security Monitoring: Collection, Detection, and Analysis, 1st Ed. Ed., Elsevier [ISBN: 9780124172081]