ROBERT GORDON UNIVERSITY ABERDEEN

MODULE DESCRIPTOR

Module Title

Securing Networks

Reference	CM2135	Version	1
Created	November 2023	SCQF Level	SCQF 8
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module emphasises securing computer networks by exploring fundamental principles and applying practical security methodologies.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Show competence in the basic principles of network security.
2	Show awareness of various network attacks applicable to modern computer networks.
3	Compare various network security measures to pinpoint the optimal approach for securing a given network scenario.
4	Implement robust security measures to protect networks.

Indicative Module Content

Security Overview: Encompassing security goals, Network types and security measures, attacker models, networking applications, network protocols, security tools, and various network security topics. Communication Security Protocols: Delving into TLS (Transport Layer Security),TCP security, UDP security, IPv4 and IPv6 security, routing security, ICMP security, IP spoofing, and fragmentation attacks. Network Infrastructure Security: Discussing VPNs and IPsec, NAT, security within and across autonomous systems, port-based Network Access Control (IEEE 802.1X), WAN link-layer security, attacks on Ethernet switches, ARP/NDP protocols, network segmentation, firewalling, network security monitoring, and network access control. Security Measures and Technologies: network infrastructure, devices, security architecture, authentication, authorization, auditing, intrusion prevention, virtual private networks, and network attacks (physical interception, ARP spoofing, DNS poisoning, IP spoofing, DHCP starvation, rogue servers, packet sniffing, DoS/DDoS, Man-in-the-middle). Wireless Security and Attacks at Layer 2: Addressing wireless cracking, rogue wireless access points, and network security monitoring, along with attacks and mitigation at Layer 2 (MAC/ARP spoofing, overflow attacks, VLAN storms, STP attacks).

Module Ref:	CM2135 v1

Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Coursework consisting of both practical and theoretical elements covering all module learning outcomes.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM1132: Computer Network Fundamentals or equivalent prior learning
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CM2135 v1

INDICATIVE BIBLIOGRAPHY

1	Stallings, W. (2022). Network Security Essentials: Applications and Standards. Pearson.
2	Kaufman, C., Perlman, R., & Speciner, M. (2023). Network Security: Private Communication in a Public World. Pearson.
3	Shimeall, T., & Spring, J. (2019). Introduction to Computer and Network Security: Navigating Shades of Gray. Wiley.
4	Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley