ROBERT GORDON UNIVERSITY ABERDEEN

MODULE DESCRIPTOR

Module Title

Network Security

Reference	CMM528	Version	8
Created	January 2023	SCQF Level	SCQF 11
Approved	May 2013	SCQF Points	15
Amended	June 2023	ECTS Points	7.5

Aims of Module

To provide the student with the ability to identify and analyse network security threats. To provide students with the necessary skills to design and manage secure networks.

Learning Outcomes for Module

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

1	Demonstrate a critical understanding of the principles of Secure Network Design.
2	Utilise appropriate tools and techniques to protect networks against modern security threats.
3	Critically appraise the methods and technologies that can be used for network security monitoring.
4	Apply a range of specialised skills and techniques to investigate and analyse network security threats.

Indicative Module Content

Principles of secure network design. Network and endpoint device security: vulnerabilities and protective measures, Layer 2 security (MAC/ARP spoofing, overflow attacks, VLAN storms and STP attacks). Network protective measures: IPv4/IPv6 security, VPNs and IPSec, NAT. TCP/IP protocol stack: Security at the Application, Transport, Internet and Link layers. Firewall Technologies: Access Control Lists (ACLs), Zone-Base Policies, Firewalls to mitigate network attacks. Intrusion Detection and Prevention Systems (IDS/IPS): Functions and operations of Intrusion Detection/Prevention Systems, IDS/IPS signatures and alarms, signature and anomaly-based detection. Network Security Monitoring: SIEM, flow monitoring, network forensics, honeypots. Threat Hunting and Analysis: Incident response and log analysis.

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

Module Ref:	CMM528 v8

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	30
Non-Contact Hours	120	120
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
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:	This coursework consists of a threat investigation and secure network design.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the 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	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM528 v8

INDICATIVE BIBLIOGRAPHY

1	McNAB,C., 2016. Network Security Assessment. O'Reilly.3rd Ed.
2	BIJALWAN, A., 2022. Network forensics: privacy and security. Chapman & Hall/CRC Press.
3	MURDOCH, D., 2019. Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independently published.
4	KIZZA, 2017. Guide to Computer Network Security. Springer.
5	STALLINGS, 2017. Network Security Essentials: Applications and Standards. Pearson
6	BHUYAN, M., BHATTACHARYYA, D., and KALITA, J., 2017. Network traffic anomaly detection and prevention: concepts, techniques, and tools. Springer.