Title	Secure Systems Architecture
Long Title	Secure Systems Architecture
Credits	**5**
NFQ Level	**Expert**

Module Description:

In this module students will learn how to write programs and scripts to perform cyber security functions such as packet manipulation and network scanning techniques. In addition, they will learn ethical hacking techniques to program a range of network, web and malware attacks with the aim of evaluating and identifying vulnerabilities in systems and networks.

Learning Outcomes

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

LO1 Evaluate the applicability and use of Cybersecurity Architecture Frameworks to support and implement secure systems in an organisation.

LO2 Evaluate factors driving the need for network security and assess how network security techniques are implemented as preventive measures to provide robustness to example points of vulnerability and attacks.

LO3 Appraise and apply cybersecurity controls and techniques in the design of organisation's system architecture to meet confidentiality, integrity and availability (CIA) requirements.

LO4 Critically assess the security of a cloud based virtualized architecture with the aim of protecting data, application and services in a cloud computing architecture

LO5 Apply cybersecurity controls to achieve defence in depth (DiD) to protect the confidentiality, integrity, and availability of the data within a system

Indicative Content

Frameworks for Enterprise Security Architecture

SABSA - Enterprise Security Architecture. Cross Boundary Enterprise Security Framework (CB ESM). Cybersecurity Operations Centre (CSOC). The Open Group Architecture Framework (TOGAF). Critical review and comparison of different frameworks.

Cloud Computing

Security Architecture and Networking Technologies as they apply and are used in the Cloud. Policies, technologies and control to protect cloud resources. Data Centres, Virtualisation, Data Containers, Automation, Micro-segmentation. Cloud-based attacks (Cryptojacking, E-skimming, Unauthorised Access) and security mechanisms (Network, Cloud Instance, DevSecOps, Containerization, Applications, File Storage, Conformity and Governance). The need for security design implementation builtin at the beginning of the design process, so as to guarantee a stronger and less vulnerable system architecture.

Security Controls

Access control and authentication mechanisms. Permissions and the role of authentication in access controls. Authentication mechanisms. Cryptography basic's and its various applications.

Security Technologies and Products

Firewalls, IPS/IDS, DLP, SIEM, Log Correlation and Management, UTM, User and Entity Behaviour Analytics (UEBA), Honeypots, Network Traffic Analysis, Threat Feeds, Next Generation, Anti-Virus, Patch Management, Change Management, Perimeter Management, Web Security, Email Security, Server Security, Defence in Depth, SOC, NOC, Network Monitoring Devices. Deployment of these to prevent and detect attacks to protect runtime physical, virtual, and cloud systems.

Network Security Concepts

Forms of attacks on data networks (Passive and Active), Potential Network Vulnerabilities, Connection and Connectionless transmission, Transmission medium, Data Packet concepts - Frame Check Sequence, Encryption (where it can be used), Message Integrity Codes, Forward Error Correction, DSSS, FHSS, CDMA. The associated performance metrics and restrictions that may apply to the use of such security concepts such as small packet size, low bandwidth, high transmission costs, limited processing and storage resources and real-time constraints. Policies, processes and practices that are adopted to secure a network by detecting, preventing and monitoring attacks.

Product Security Architecture

Designing software with security in mind. Where security controls fit into software design and development. Secure Software Development Lifecycle, including CICD pipelines. Privacy by Design. Protecting IP in software products. Managing third party and technology partner ecosystem risks. Chip-to-Cloud Security. Secure product support, OWASP Top 10, Web App Firewalls, Security of containers

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Students are presented with a case study referring to a hypothetical or actual attack on an organisation's IT system are expected to consider the impact of the attack in violating its security requirements at a business, regulatory and customer level, in addition to how proper governance could have been used to protect the confidentiality, integrity and availability of the system.	1,2,	40	Week 8
Project	Students assess and design a range of security controls to achieve defence in depth (DiD) to protect information confidentiality, integrity and availability (CIA) for a system which includes cloud based virtualized infrastructure. Students present their findings and designs through a written report or oral presentation.	3,4,5	60	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	Lectures covering the theoretical concepts underpinning the subject.	2	Every Week	2.00
Lab	Lectures covering the theoretical concepts underpinning the subject.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student including preparing project deliverables and reading resource materials.	3	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	Lectures covering the theoretical concepts underpinning the subject.	2	Every Week	2.00
Lab	Labs to apply techniques learned to realistic case studies.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student including preparing project deliverables and reading resource materials.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

- **Neil Rerup and Milad Aslaner 2018, Hands-On Cybersecurity for Architects : Plan and Design Robust Security Architectures, Packt Publishing [ISBN: 9781788830263]**