NETW H4209: Network Security

Module Title:	Network Security
Credits:	10
NFQ Level:	8
Module Delivered In	No Programmes
Teaching & Learning Strategies:	A mix of traditional lectures, laboratory work and take-home projects will enable the learner to fully understand and practice the various networking concepts presented.
Module Aim:	To provide the learners with the knowledge and skills to design, configure, maintain and troubleshoot a secure network.

Learning Outcomes	
On successful completion of this module the learner should be able to:	
LO1	Critique the primary security threats to network and information security.
LO2	Validate secure access with Authentication, Authorisation and Accounting (AAA).
LO3	Design, configure and evaluate firewalls to mitigate network attacks.
LO4	Design, implement and evaluate Intrusion Detection and Prevention Systems (IDPS) to mitigate network attacks.
LO5	Evaluate wired and wireless LAN vulnerabilities and justify protective measures.

Pre-requisite learning		
Module Recommendations *This is prior learning (or a practical skill) that is recommended before enrolment in this module.*		
7079	ZNTW H3201	Networking III
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module.*		
No incompatible modules listed		
Co-requisite Modules		
No Co-requisite modules listed		
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.*		
No requirements listed		

NETW H4209: Network Security

Module Content & Assessment

Indicative Content
Security Treats (20%): Attack methodologies; Viruses, worms and Trojan horses; Principles and features of a secure network; Securing network devices
Authentication, Authorisation and Accounting (AAA) (20%): Local and server based authentication, server based authorisation and accounting (e.g. RADIUS and TACACS+)
Firewalls (15%): Review ACLs, Configure firewalls, Implement and evaluate zone-based policy firewalls, Context-based Access Control (CBAC), DMZ
Log File and Traffic Analysis (10%): Read, translate and analyse logs generated for event; Traffic monitoring and analysis
IDPS (15%): Types of IDPSs (e.g. Network IDPSs, Anomaly-based IDPS, Signature-based IDPS), IPS Evasion Techniques (e.g. Evader: Encryption and Tunnelling, Timing Attacks, Resource Exhaustion, Traffic Fragmentation, Protocol-level Misinterpretation), Anti-evasion countermeasures
Wired and Wireless LAN Security (20%): Endpoint vulnerabilities and protective measures, Layer 2 vulnerabilities and security measures, Switch security features (e.g. Port Stealing, Switch flooding, storm control), rogue Access Points and devices, man-in-the-middle attacks

Assessment Breakdown	%
Continuous Assessment	20.00%
Practical	30.00%
End of Module Formal Examination	50.00%

Continuous Assessment

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Examination	n/a	1,2,3	10.00	Week 19
Examination	n/a	4,5	10.00	Week 28

No Project

Practical

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Practical/Skills Evaluation	Weekly practical/laboratory work is designed to allow students to demonstrate the achievement of all the learning outcomes.	1,2,3,4,5	15.00	n/a
Practical/Skills Evaluation	Practical Examination	1,2,3,4,5	15.00	Week 29

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	n/a	1,2,3,4,5	50.00	End-of-Semester

SETU Carlow Campus reserves the right to alter the nature and timings of assessment

NETW H4209: Network Security

Module Workload

Workload: Full Time		
Workload Type	*Frequency*	*Average Weekly Learner Workload*
Lecture	Every Week	2.00
Laboratory	Every Week	2.00
Estimated Learner Hours	Every Week	2.66
	Total Hours	6.66