



TEQSA ID PRV:14323
CRICOS Provider Code: 03866C

MIT602 NETWORK SECURITY

SYDNEY INSTITUTE OF HIGHER EDUCATION > PROGRAMS > MIT602 NETWORK SECURITY

Unit Outline

Important Update:	Our aim is to provide you with an optimal learning experience, regardless of how this unit is delivered. Teaching will be delivered in line with the most current COVID Safe health guidelines. This may include a mix of online and face-to-face. Please check the learning management system for announcements and updates. Thank you for your flexibility and commitment to studying with Sydney Institute of Higher Education.
Enrolment Modes:	Year 2, Semester 1.
Credit Point(s):	12.5
EFTSL Value:	0.125
Prerequisites:	MIT504 Networking , MIT508 BIT101
Typical study commitment:	Students will on average spend 10 hours per week over the teaching period undertaking the teaching, learning and assessment activities for this unit.
Scheduled learning activities:	4 timetabled hours per week, 6 personal study hours per week.
Other resource requirements:	Students will need access to lab computers or will need their own laptops in order to carry out lab exercises and assignments. Packet Tracer and Kali Linux are needed for this unit.

Unit description

This unit is an in-depth exploration of the principles, methodologies, and technologies essential for safeguarding information within computer networks. This unit covers a spectrum of topics crucial to understanding and mitigating network security threats, including cryptographic protocols, access controls, wireless network security and network security policies. The unit also addresses the dynamic nature of network security, exposing students to emerging threats, attack vectors, and vulnerability assessment techniques. Students will gain hands-on experience in implementing security measures and developing strategies to mitigate potential risks. By the end of the unit, students will have a solid understanding of how to design, implement, and manage effective security measures to protect information assets within a networked environment.

Unit learning outcomes (ULO)

On the successful completion of this unit student will be able to:

ULO1	Demonstrate why networks are vulnerable to abuse and destructions.
ULO2	Develop and gain an advanced level of Cryptography understanding.
ULO3	Analyse common threats, attacks, mitigation of network systems.
ULO4	Explain the major methodologies to secure network systems.
ULO5	Analyse and discuss common authentication and access management.
ULO6	Evaluate and explore the vulnerability and risk mitigation.

Topics to be included in the unit

1.	Introduction to Network Security
2.	Threats and Attacks on Endpoints
3.	Basic Cryptography
4.	Advanced Cryptography,
5.	Networking Threats, Assessments, and Defenses
6.	Network Security Appliances and Technologies
7.	Administering Secure Networks
8.	Wireless Network Security
9.	Mobile Device Security
10.	Authentication
11.	Risk Management and Data Privacy
12.	Revision

Assessment

Assessment Description	Grading and weighting (% total mark for unit)	Due date
Assessment 1: Weekly Lab	20%	Weeks 1-10
Assessment 2: Mid-Semester Exam	10%	Mid-semester week
Assessment 3: Technical Report (Group)	30%	Week 12
Assessment 4: Final Exam	40%	Final exam week