



DUBLIN INSTITUTE OF TECHNOLOGY

**DT211C/4 BSc. (Honours) Degree in Computer
Science (Infrastructure)**

DT228/4 BSc. (Honours) Degree in Computer Science

**DT282/4 BSc. (Honours) Degree in Computer Science
(International)**

SUMMER EXAMINATIONS 2017/2018

ADVANCED SECURITY 2 [CMPU4008]

DR. ANEEL RAHIM

DR. DEIRDRE LILLIS

DR. DAVID MALONE – DT211C

MR. PATRICK CLARKE – DT228/DT282

TUESDAY 8TH MAY

2.00 P.M. – 4.00 P.M.

DURATION

2 HOURS

INSTRUCTIONS TO CANDIDATES

ANSWER **THREE** QUESTIONS OUT OF **FOUR**.

ALL QUESTIONS CARRY EQUAL MARKS.
ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

1. (a) Explain any four Google advance operators that can be used by a hacker to exploit sensitive information. Use an example to compliment your answer. (10 marks)

(b) Define the user authentication process and briefly explain the password based authentication and mention the different attacks against it. (13 marks)

(c) Define Biometric Authentication and describe the physical characteristics used for biometric identification. (10 marks)

2. (a) Explain the UNIX File Access Control. (10 marks)

(b) Explain the Discretionary Access Control (DAC) and Draw the Access Matrix, Access Control List and Capability List (13 marks)

(c) Describe three countermeasure for SQL injection Attacks. (10 marks)

3. (a) Describe the different types of cloud security attacks and what can be done to defend against these types of attacks. (12 marks)
- (b) What steps should be taken in order to prevent the denial of service (DoS) attack? (9 marks)
- (c) In context of DoS attack, explain the Reflection attack and Amplification attack. (6 marks)
- (d) Explain the macro virus, encrypted virus and polymorphic virus. (6 marks)
4. (a) In context of malware, explain the backdoor, keylogger, spyware, and a rootkit? (8 marks)
- (b) Discuss the desirable characteristics of an Intrusion Detection System. (9 marks)
- (c) What is a honeypot and briefly define the two types of honeypots that may be deployed. (8 marks)
- (d) Define the intrusion prevention system (IPS) and explain the host-based IPS and network-based IPS. (8 marks)