DUBLIN INSTITUTE OF TECHNOLOGY

DT211C BSc. (Honours) Degree in Computer Science (Infrastructure)

DT228 BSc. (Honours) Degree in Computer Science

Year 4

SUMMER EXAMINATIONS 2016/2017

ADVANCED SECURITY 2 [CMPU4008]

DR. ANEEL RAHIM
DR. DEIRDRE LILLIS
MR. THOMAS NOLAN

WEDNESDAY 17TH MAY   1.00 P.M. – 3.00 P.M.

TWO HOURS

INSTRUCTIONS TO CANDIDATES

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

ALL QUESTIONS CARRY EQUAL MARKS.

1. **(a)** Describe the basic concept of a challenge-response protocol for remote user authentication. Use a diagram to illustrate your answer. (13 marks)

(b) The Google operators can be considered as hackers' weapons. Explain how an hackers could exploit information using the following: (10 marks)

    i.   filetype:xls username password email
    ii.   Allinurl: cgi-bin password
    iii.   Intext: Administrator login
    iv.   inurl:admin backup
    v.   cache: www.dit.ie

(c) List and briefly describe four common strategies for passwords selection (10 marks)

2. **(a)** Describe the Role based Access model and mention the three types of role hierarchy constraints. (13 marks)

(b) Describe the Attribute-Based Access Control model. Use a diagram to illustrate your answer. (10 marks)

(c) Describe some of the main cloud-specific security threats. (10 marks)

3. **(a)** Define a denial-of-service (DoS) attack and what types of resources are targeted by

    such attacks. (8 marks)

   (b) Describe the different type of flooding attacks? (6 marks)

   (c) List and briefly define four classes of intruders. (12 marks)

   (d) Define intrusion detection and describe the three logical components of an intrusion

    detection system. (7 marks)

4. **(a)** Describe the malware countermeasure approaches. (7 marks)

   (b) Describe the virus classification on the basis of target and strategy. (6 marks)

   (c) List and briefly define four different types of firewall. (12 marks)

   (d) Describe the four firewall filter characteristics that are used by firewalls to control

    access and enforce a security policy. (8 marks)