Office Use Only

MONASH University

Semester Two 2021
Examination Period

Faculty of Information Technology

EXAM CODES: **FIT 5037 (sample test)**

TITLE OF PAPER: Network Security

EXAM DURATION: 2 hours 10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT: (tick where applicable)

☐ Caulfield ✓Clayton ☐ Parkville ☐ Peninsula
☐ Monash Extension ☐ Off Campus Learning ☐ Malaysia ☐ Sth Africa
☐ Other (specify)

During an exam, you must not have in your possession any item/material that has not been authorised for your exam. This includes books, notes, paper, electronic device/s, mobile phone, smart watch/device, calculator, pencil case, or writing on any part of your body. Any authorised items are listed below. Items/materials on your desk, chair, in your clothing or otherwise on your person will be deemed to be in your possession.

No examination materials are to be removed from the room. This includes retaining, copying, memorising or noting down content of exam material for personal use or to share with any other person by any means following your exam.

Failure to comply with the above instructions, or attempting to cheat or cheating in an exam is a discipline offence under Part 7 of the Monash University (Council) Regulations, or a breach of instructions under Part 3 of the Monash University (Academic Board) Regulations.

AUTHORISED MATERIALS

OPEN BOOK	☐ **YES**	✓ **NO**
CALCULATORS	☐ **YES**	✓ **NO**
SPECIFICALLY PERMITTED ITEMS	☐ **YES**	✓ **NO**

if yes, items permitted are:

Candidates must complete this section if required to write answers within this paper

STUDENT ID: _ _ _ _ _ _ _ _ _ DESK NUMBER: _ _ _ _ _ _

Final test contents: 7 questions, 30 marks total.

PART A (2.5 marks)

TRUE/FALSE questions (final exam will contain 5 questions)

1. A loss of integrity is unauthorised modification of data during the communication.

   a) True
   b) False

2. IPSec encapsulation mode provides protection to the entire IP packet.

   a) True
   b) False

3. Machine learning based intrusion detection systems are likely to produce false positives during traffic analysis.

   a) True
   b) False

4. DDoS attacks cannot be launched at the application layer.

   a) True
   b) False

PART B (2.5 marks)

Single-choice questions. (final exam will contain 5 questions)

1. Which of the following is an example aspect of network security?
   a) wireless security
   b) physical security
   c) human input errors

2. **Ciphertext-only** capability means that: _____.
   a) only decryption can be performed on the ciphertexts
   b) the adversary can only access to the ciphertexts
   c) the adversary can only decrypt chosen ciphertexts

3. PGP provides **confidentiality** through the use of _____.
   a) symmetric block encryption
   b) radix-64
   c) digital signatures

4. In IPSec, authentication NOT applied to the entire original IP packet is _____.
   a) cipher mode
   b) transport mode
   c) tunnel mode

PART C (25 marks)

(final exam will contain 7 questions)

Q1. (5 marks) Intrusion detection system (IDS) is a software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted/malicious activities.

a) List and explain at least 2 design goals of an intrusion detection system. (2 marks)

b) What are Signature-based detection and Anomaly-based detection? Please briefly explain the two detection approaches, respectively. (2 marks)

c) Compared with Anomaly-based detection, what are the strength and weakness of Signature-based detection in the real-world applications. (1 marks)

Q2. (5 marks) In the following figure, an attacker aims to launch the TCP flooding attack to create network congestion to a server.

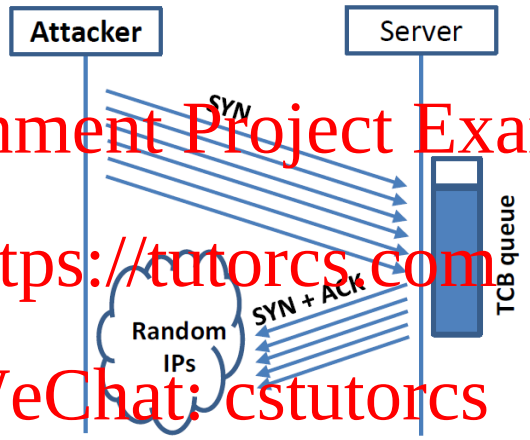

Figure: TCP Flooding Attack Scenario

a) Please explain how the attacker shown in the above figure can launch the TCP flooding attack. (1 marks)

b) Please list one countermeasure that can defend against the TCP flooding attack (1 marks). Then explain how they can effectively address the attack, respectively (1 marks).

c) If the server does not allocate any resource to maintain the connections during the TCP handshake, will the attack still be successful? (1 marks) What could be a possible issue introduced by this approach? (1 marks)