



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

COURSE	:	COMPUTER SECURITY
COURSE CODE	:	CSC662
EXAMINATION	:	OCTOBER 2026 (MOCK)
TIME	:	3 HOURS

MARKING SCHEME NOTES

1. This marking scheme accompanies the CSC662 mock paper (October 2026).
Computed answers show working; theory answers are supported by lecture slides (not lecturer-marked); verbatim quotes are omitted in this public build; slide citations are retained.
2. Supported theory marking points quote the lecture decks; any unresolved slot would remain a visible placeholder.
3. Part A = $10 \times (2 + 6)$; Part B = $2 \times (5 + 5)$; total = 100 marks.
4. Computed: 3 slot(s). Supported theory: 19 slots. Placeholders: 2.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of 14 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

Labels: computed / supported by lecture slides (not lecturer-marked) / placeholder. No official marking scheme exists for the real CSC662 papers; this is generated for the mock.

Entailment labels: supported = the private quote directly supports the point (or the point passed the stem-overlap gate); partly supported = partial/ambiguous support; not supported = no support. Quote text is omitted here; verdicts come from private verification.

Part A: $10 \times (2 + 6) = 80$ marks. Part B: $2 \times (5 + 5) = 20$ marks. Total: 100 marks. Slots: 3 computed, 19 supported by lecture slides, 2 placeholder.

Methods: computed answers use verified solvers. Theory answers are supported by lecture slides (not lecturer-marked). Each point carries a deck/slide citation and overlap score; verbatim quote text is omitted from this public build. Low overlap is flagged for human review.

PART A - QUESTION 1

A1a - 2 marks - computed - matches lecture slides 5-9 (Caesar shift 3 examples)

Question:

Using Caesar Cipher technique, decrypt the following ciphertext with a shift of 7 (replace each letter with the one 7 positions to the left).

KLCPJLYLABYULKHUKDPWLKVUL

Answer: DEVICERETURNEDANDWIPIEDONE

Working:

```

K (10) -7 mod 26 -> D
L (11) -7 mod 26 -> E
C ( 2) -7 mod 26 -> V
P (15) -7 mod 26 -> I
J ( 9) -7 mod 26 -> C
L (11) -7 mod 26 -> E
Y (24) -7 mod 26 -> R
L (11) -7 mod 26 -> E
A ( 0) -7 mod 26 -> T
B ( 1) -7 mod 26 -> U
Y (24) -7 mod 26 -> R
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
H ( 7) -7 mod 26 -> A
U (20) -7 mod 26 -> N
K (10) -7 mod 26 -> D
D ( 3) -7 mod 26 -> W
P (15) -7 mod 26 -> I
W (22) -7 mod 26 -> P
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
V (21) -7 mod 26 -> O
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E

```

Suggested marks: 1 mark for identifying the cipher/shift direction; 1 mark for the complete plaintext.

Confidence: computed - matches lecture slides 5-9 (Caesar shift 3 examples).

A1b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

State six facts about substitution ciphers as presented in the lecture, covering what the cipher does to plain-text letters, what serves as the key, the resulting output, the Shannon principle it corresponds to, and where the idea is applied today.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The cipher works by swapping each plain-text letter for a different letter.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.67
2	The text produced after the replacement is called the cipher-text.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.33 LOW
3	The rule used to perform the substitution acts as the key.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.50
4	This substitution mechanism maps onto Shannon's confusion principle.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.43 LOW
5	The same substitution concept carries over into contemporary cipher designs.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.11 LOW
6	Vigenere's polyalphabetic scheme extends the Caesar shift cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 14 031 - Classical Cryptography::s14::1	supported (stem gate)	0.71

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 031 - Classical Cryptography, slide 14; 031 - Classical Cryptography, slide 4

PART A - QUESTION 2

A2a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

List two facts about transposition ciphers as described in the lecture, covering how the rail fence cipher arranges plain-text and what serves as its key.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The rail fence cipher writes the plain-text in a zigzag pattern across rows and then reads letters off row by row to form the cipher-text.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 25 031 - Classical Cryptography::s25::1	supported (stem gate)	0.67
2	The key of a rail fence cipher is a positive integer giving the number of rows.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 25 031 - Classical Cryptography::s25::1	supported (stem gate)	0.86

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 031 - Classical Cryptography, slide 25

A2b - 6 marks - computed - matches lecture slide 15 (standard tableau)

Question:

Decrypt the following ciphertext using the Vigenere cipher with the key CIPHER. Use the standard 26 x 26 Vigenere tableau, writing the key over the message and repeating it as necessary.

UMRBVVNWVPREQE

Answer: SECURELOGINNOW

The 26 x 26 Vigenere tableau is printed in the question paper.

Working:

Standard 26 x 26 tableau, A=0; key repeated over the ciphertext.

Ciphertext: UMRBVVNWVPREQE

Key: CIPHERCIPHERCI

Letter-by-letter: C - K mod 26 = P

U (20) - C (2) = 18 -> S

M (12) - I (8) = 4 -> E

R (17) - P (15) = 2 -> C

B (1) - H (7) = 20 -> U

V (21) - E (4) = 17 -> R

V (21) - R (17) = 4 -> E

N (13) - C (2) = 11 -> L

W (22) - I (8) = 14 -> O

V (21) - P (15) = 6 -> G

P (15) - H (7) = 8 -> I

R (17) - E (4) = 13 -> N

E (4) - R (17) = 13 -> N

Q (16) - C (2) = 14 -> O

E (4) - I (8) = 22 -> W

Plaintext: SECURELOGINNOW

Suggested marks: 1 mark for the key/table setup; 4 marks for the letter-by-letter working; 1 mark for the complete answer.

Confidence: computed - matches lecture slide 15 (standard tableau).

PART A - QUESTION 3

A3a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

List the stages that make up the identification stage and the authentication stage of a biometric authentication process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage begins with acquisition of the biometric sample.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.50
2	The identification stage also includes storing the master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.17 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 5

A3b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Refer to your answer in (a). Based on the scenario in (a), discuss the biometric mechanisms and technologies used for authentication. Your discussion should cover the definition of a biometric, the two categories of biometric applications, and specific technologies with their characteristics.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A biometric is defined as a physiological or behavioural characteristic of a human being that can distinguish one person from another and can theoretically be used for identification or verification of identity.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.92
2	Biometric applications are categorized into two sectors: psychological (physiological) and behavioural.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.62
3	The psychological category includes iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.78
4	The behavioural category includes voice, typing pattern and signature.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.67
5	Retinal scanning is very efficient and cannot be spoofed, but has disadvantages such as the user having to look directly, a high FTE ratio, acceptability concerns, light exposure and hygiene.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 9 072 - Biometrics and Authentication::s09::1	partly supported	0.14 LOW
6	Iris scanning scans a unique pattern of the iris, requires no touch, and overcomes retinal scanner issues, although contact lenses may be an issue.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.29 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 9

PART A - QUESTION 4

A4a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain the Chinese Wall model as a formal security model, covering the policy it implements and how its access rules behave over time.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall is a confidentiality access control policy (not an integrity policy) that addresses conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.55

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Access rights change dynamically because they depend on the subject's history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.80

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 24

Status: computed placeholder - no question generated for this type.

PART A - QUESTION 5

A5a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain the difference between morals, ethics and laws as they apply to the conduct of a computing professional.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct, forming the basis of social behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.55
2	Laws are formal rules of conduct imposed by a sovereign authority such as a government on its subjects or citizens.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	1.00

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 071 - Ethics and Computer Security, slide 5

A5b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

State six professional conduct requirements that the ACM code places on a computing professional, covering both how they carry out their work and how they treat the public and the systems they build.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A professional must aim for high quality in the processes and products of their professional work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.75
2	A professional must keep up high standards of competence, conduct and ethical practice.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.78
3	A professional must only perform work in areas where they are competent.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	A professional must give thorough evaluations of computer systems and their impacts, including possible risks.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.80
5	A professional must contribute to society and human well-being, recognising that all people are stakeholders in computing.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.73
6	A professional must respect privacy and honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.50

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12

PART A - QUESTION 6

A6a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) typical locations where IDS sensors are placed in a network-based IDS architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be positioned just inside the firewall.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.50
2	A sensor can be positioned on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.25 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 062 - Intrusion Detection System, slide 7

A6b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Describe six (6) preventive network security mechanisms and the protection each provides, as covered in the network security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing network traffic according to predetermined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
2	A proxy server improves data security and network performance by acting as a firewall and web filter, sharing connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.79

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Network segmentation creates boundaries between segments whose computing assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.77
4	A remote access VPN gives individual hosts or clients remote and secure access to an organization's network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access (ZTNA) restricts a user to only the access and permissions needed to fulfil the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.50
6	Intrusion detection/prevention systems detect or prevent attacks such as brute force, denial-of-service and exploitation of network vulnerabilities.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.85

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 061 - Network Security, slide 3; 061 - Network Security, slide 4

PART A - QUESTION 7

A7a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) points about software insecurity and buffer overflows as described in the Software Security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Software insecurity arises because attackers can alter resources that are critical for program execution, such as the instruction pointer or function call addresses.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.65
2	A buffer overflow occurs when, lacking proper bound checking, buffer content spills into adjacent higher stack memory and lets an attacker overwrite the return address to hijack execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	partly supported	0.35 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples n<3; widened via topic+marks (any command).

Citations: 051 - Software Security, slide 21; 051 - Software Security, slide 30

A7b - 6 marks - PLACEHOLDER

Topic: software/OS security; command: Explain

Status: placeholder - no supported question passed verification.

Reason: A7b point 1: marking point is a verbatim copy of its quote; phrase the point as an answer requirement, not as copied slide text

PART A - QUESTION 8

A8a - 2 marks - PLACEHOLDER

Topic: access control models; command: State

Status: placeholder - no supported question passed verification.

Reason: A8a: sub-angle not followed; use one of ['acl', 'acm', 'capability', 'access control list', 'matrix']

A8b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

*Discuss the goals of access control and the role of the reference monitor in authorization, and explain how the Chinese Wall model's simple security rule and *-property constrain access over time. Provide six distinct points.*

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that access control aims to grant, limit, prevent, and revoke access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.86
2	Explain that the reference monitor is the component that makes authorization decisions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	1.00
3	Note that reference monitors realize access control policies and can be deployed at all levels of the system hierarchy.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	0.92
4	Describe the Chinese Wall simple security rule: access is granted only if the object is within the same company dataset already accessed or in a different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	supported (stem gate)	0.77
5	Explain the Chinese Wall *-property: write access requires simple-rule permission and no read access to unsanitized information in a different company dataset.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	supported (stem gate)	0.64
6	State that the Chinese Wall is an access control policy whose accesses depend on the history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	0.78

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 023 - Access Control and Authorization, slide 18; 023 - Access Control and Authorization, slide 4; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 26; 024 - Formal Security Model, slide 27

PART A - QUESTION 9

A9a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain two password security controls that can be applied to password files and accounts to strengthen authentication.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control should be applied to the password files themselves.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.57
2	Accounts should be de-activated after multiple failed login attempts.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.75

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 12

A9b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how single sign-on and Kerberos-based authentication mechanisms reduce the burden of password management for users in a large distributed environment, and describe the role of smart cards as an alternative authentication mechanism.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the need for users to memorize multiple passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
2	Single sign-on reduces the time users spend typing passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.43 LOW
3	Single sign-on lowers the effort required to maintain passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.29 LOW
4	Kerberos is a client-server architecture that provides single sign-on.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.57
5	In Kerberos login, the user enters a user name and password at the client workstation.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.71
6	The hash of the user's password becomes the secret key of the client.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	1.00

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 19

PART A - QUESTION 10

A10a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain two characteristics of Trojan horses as a type of malware, including how they present themselves and what harm they cause once active.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojan horses disguise themselves as useful or benign programs so users install them unsuspectingly.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.10 LOW
2	Once running, a Trojan steals private data, deletes files, logs keystrokes, or opens a way for additional malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.64

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 12

A10b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain six techniques by which malware such as viruses and worms propagate themselves or attach their code to a host program, and describe how early malware demonstrated these propagation methods.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can propagate by appending its body to a host program and saving the original entry point inside the virus body.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.58
2	A virus can replace the program entry point with a jump to the virus body, and the virus code later restores the original entry point and jumps to it.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.83
3	For EXE files, a virus can overwrite the program header so that the entry point switches to the virus, and then jump to the original entry point during execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.67
4	The Morris worm propagated across the Arpanet by exploiting a debugging feature of sendmail that allowed remote execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.55
5	Elk Cloner spread through boot sector infection and hooked the reset handler so that a poem was played on every fiftieth reset.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.71
6	The Brain virus was included in the boot sector of distributed software diskettes, which is how it spread in the wild.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.60

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 10; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART B - QUESTION 1

B1a - 5 marks - supported by lecture slides (not lecturer-marked)**Question:**

Explain five ways in which threat classes and malware can impact the confidentiality, integrity and availability of an information system, giving a distinct impact for each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure threats such as snooping, sniffing and wiretapping give unauthorised access to information, harming confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.27 LOW
2	Deception threats involve acceptance of false data, which damages integrity.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported (stem gate)	0.50
3	Usurpation threats give unauthorised control of part of a system and are countered by availability services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.44 LOW
4	Spyware steals user logins and passwords, so sensitive bank information can be compromised.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	partly supported	0.40 LOW
5	Rootkits hide malicious processes and software so that the infected computer stays under the malware author's control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.50

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 011 - Introduction to Computer Security, slide 10; 051 - Software Security, slide 13

B1b - 5 marks - supported by lecture slides (not lecturer-marked)**Question:**

The Samy worm spread through MySpace by exploiting a cross-site scripting flaw. Explain five aspects of this case: how the malicious script was injected, how the worm gathered and added friends, how infection spread to visitors, how the script reached the browser, and the eventual scale of the outbreak.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by writing to document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.70
2	It obtained the list of the user's heroes by issuing a GET request on a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.43 LOW
3	It added Samy as a friend by performing an XML-HTTP request on the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
4	Any user visiting an infected user's page had their own profile and friends list infected with the JavaScript.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.70
5	The outbreak eventually infected about 1,000,000 MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.71

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 052 - Web Security, slide 15

PART B - QUESTION 2

B2a - 5 marks - supported by lecture slides (not lecturer-marked)

Scenario:

A hospital wants every workstation to prove at boot that it is running only approved software before it is allowed to access patient records. The IT team is told to base the design on the Trusted Platform Module and a chain of trust, and to explain the components involved.

Question:

State the role of the Trusted Platform Module in a trusted platform, and explain how a chain of trust is built from the hardware up to the running software, naming the stages involved and the roots of trust that support it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The TPM is described as tamper-resistant hardware fitted into the platform.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 6 073 - Trusted Computing::s06::1	supported (stem gate)	0.57
2	The TPM's duties are listed as measurement, protected storage, integrity reporting and policy enforcement.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 6 073 - Trusted Computing::s06::1	supported (stem gate)	0.78
3	In the chain of trust, each stage measures and validates the stage that follows it.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.50
4	The measurements taken are recorded in the TPM's Platform Configuration Registers.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.71
5	The chain begins at the hardware TPM and proceeds through the RTM, TPM software stack, BIOS and kernel, ending with the whole platform verified as trusted.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.50

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 073 - Trusted Computing, slide 6; 073 - Trusted Computing, slide 8

B2b - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

Referring to the scenario, discuss the NGSCB/Nexus components that the IT team could use to enforce the approved-software requirement, covering the role of Nexus, the role of the Nexus Computing Agent, and how these components relate to the TPM.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is described as a security kernel that is authenticated on boot.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.80
2	Nexus authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.75

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Nexus provides the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.60
4	The Nexus Computing Agent is a trusted software component.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported	0.40 LOW
5	The NCA runs in a trusted mode that communicates with Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.83

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

End of marking scheme.