



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: 1 slot(s). Supported theory: 23 slots. Placeholders: 0.
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 15 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 x (2 + 6) = 80 marks. Part B: 2 x (5 + 5) = 20 marks. Total: 100 marks. Slots: 1 computed, 23 supported by lecture slides, 0 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 - supported by lecture slides (not lecturer-marked)

Question:

List TWO (2) differences between morals and laws as described in the lecture on ethics and computer security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.86
2	Laws are described as formal rules of conduct imposed by a sovereign authority such as a government.	[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.

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

Citations: 071 - Ethics and Computer Security, slide 5

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

Question:

Discuss how a professional code of ethics and conduct guides a computing professional in carrying out security-related work. Support your discussion with six (6) distinct obligations drawn from the ACM code.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The 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	The professional must uphold strong levels 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)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The 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
4	The professional must only access computing and communication resources when authorised or compelled by the public good.	[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
5	The professional must respect privacy as part of the code of ethics.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.29 LOW
6	The professional must honour confidentiality as part of the code of ethics.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.14 LOW

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 11; 071 - Ethics and Computer Security, slide 12

PART A - QUESTION 2

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

Question:

Explain how a substitution cipher works, stating what serves as the key and which of Shannon's principles it corresponds to.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The cipher works by replacing each plaintext letter with a different letter, producing the ciphertext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.43 LOW
2	The substitution rule itself acts as the key, and this corresponds to Shannon's principle of confusion.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	partly supported	0.25 LOW

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

Citations: 031 - Classical Cryptography, slide 4

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.
 UMRBVVNWWVPREQE

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: UMRBVVNWWVPREQE
 Key: CIPHERCIPHERCI
 Letter-by-letter: $C - K \bmod 26 = P$
 $U (20) - C (2) = 18 \rightarrow S$
 $M (12) - I (8) = 4 \rightarrow E$
 $R (17) - P (15) = 2 \rightarrow C$
 $B (1) - H (7) = 20 \rightarrow U$
 $V (21) - E (4) = 17 \rightarrow R$
 $V (21) - R (17) = 4 \rightarrow E$
 $N (13) - C (2) = 11 \rightarrow L$
 $W (22) - I (8) = 14 \rightarrow O$
 $V (21) - P (15) = 6 \rightarrow G$
 $P (15) - H (7) = 8 \rightarrow I$
 $R (17) - E (4) = 13 \rightarrow N$
 $E (4) - R (17) = 13 \rightarrow N$
 $Q (16) - C (2) = 14 \rightarrow O$
 $E (4) - I (8) = 22 \rightarrow W$
 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:

Explain the Chinese Wall model as a formal security model, stating the concern it addresses and how its access decisions differ from static policies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy was proposed by Brewer and Nash to address 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)	1.00
2	Access decisions depend on the subject's history of past accesses, so permissions change dynamically.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported	0.33 LOW

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 27

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

Question:

Describe the access control matrix, the access control list and the capability list as access control structures, giving for each structure one advantage and one disadvantage, and state two requirements that any access control structure must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is identified as a basic control structure whose advantages are clarity of definition and ease of verification.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.27 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The access control matrix is noted to scale poorly and to handle changes poorly.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.38 LOW
3	An ACL is described as an object-centred description of access rights, which gives easy access to the access rights of an object.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.71
4	The ACL approach is criticised for giving a poor overview of access rights per subject and for making revocation difficult.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.58
5	Capability lists are named as one of the mechanisms for implementing access policies, alongside the access control matrix and ACLs.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.56
6	A required property of access control structures is the ability to express control policies together with verifiability of correctness.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.46 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: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 7; 023 - Access Control and Authorization, slide 8

PART A - QUESTION 4

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

Question:

Explain two characteristics of Trojan horse malware, including how it disguises itself and what harm it can cause once active.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves by appearing to be useful or benign software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Once running, a Trojan can steal private data, delete files, log keystrokes, or open a way for further malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.67

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

Citations: 051 - Software Security, slide 12

A4b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

State six techniques or behaviours by which malware propagates itself or conceals its activity on an infected system, drawing on the historical and technical examples covered in the course.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can spread by infecting the boot sector of a disk, as with Elk Cloner which spread via boot sector infection.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.50
2	A worm can propagate across a network by exploiting a remote execution feature of a service, as the Morris worm did with sendmail.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported	0.25 LOW
3	A virus can append its body to a program and redirect the program entry point to the virus code, restoring the original entry point afterwards.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	partly supported	0.42 LOW
4	A virus can overwrite a program header so that the entry point switches to the virus, 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	partly supported	0.46 LOW
5	A rootkit hides malicious processes and software so that the infected machine stays under the author's remote control, and it is hard to detect because it hides from detection software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	partly supported	0.40 LOW
6	Spyware secretly collects user information such as logins, passwords, visited sites and keystrokes, and can redirect the browser to unwanted sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::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 13; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART A - QUESTION 5

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

Question:

State TWO (2) typical locations where network-based IDS sensors should be placed to protect an organization's most valuable assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be placed 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 placed 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

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

Question:

Refer to your answer in (a). Based on the scenario in (a), explain how the organization can strengthen its preventive network security mechanisms by describing the role of a firewall, a proxy server, and network segmentation in controlling and protecting network traffic.

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.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.73
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 secure remote access to the 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 grants a user only the access and permissions needed to fulfill the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.55
6	IDS/IPS complement these preventive mechanisms by detecting or preventing attacks such as brute force, Denial-of-Service, and exploits of network vulnerabilities.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.73

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 6

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

Question:

Explain two ways in which a documented code of ethics shapes the ethical conduct of computing professionals in security-related work.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	It sets out a written record of which behaviours are acceptable for the professional or social group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.56
2	It makes clearer what the accepted standards of behaviour are.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.40 LOW

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 6; 071 - Ethics and Computer Security, slide 8

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

Question:

Explain six responsibilities that a computing professional owes to users and the organisation when handling private data in security-related work, drawing on the lecture's discussion of ethics and professional conduct.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Recognise that users and information specialists carry definite duties to act within ethical, moral and legal limits when handling data.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.50
2	Accept that merely describing the moral and ethical dimensions of ICT is insufficient for responsible practice.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.44 LOW
3	Follow the code of ethics and professional conduct published by the Association of Computing Machinery.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.78
4	Recognise that professional bodies such as the ACM publish a code of ethics and professional conduct that practitioners can follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported	0.42 LOW
5	Consult the IEEE Computer Society code as a further professional standard governing conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.30 LOW
6	Recognise that professional bodies such as the ACM, AITP, IEEE-CS and PMI each publish codes of ethics and professional conduct that practitioners can follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.33 LOW

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 3; 071 - Ethics and Computer Security, slide 7

PART A - QUESTION 7

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

Question:

List two classes of threats described in the course and, for each, state the security objective that is affected and the type of harm it represents.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class involving unauthorized access to information, which harms confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.44 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Deception is a threat class involving acceptance of false data, which harms integrity.	[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

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

A7b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Describe the Samy worm as a case study of a cross-site scripting attack. In your answer, explain how the malicious script was injected, how it spread between users, how the victim's browser was made to act, and the scale of the resulting infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The attacker 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	The script 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	0.38 LOW
3	The script 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)	0.70
4	Any user visiting an infected profile had their own profile and friends list infected, so the worm spread from visitor to visitor.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW
5	The victim's browser executed the malicious script contained in the response, sending the victim's cookies to the attacker's server.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 16 052 - Web Security::s16::1	supported (stem gate)	0.91
6	The infection eventually reached 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.

Citations: 052 - Web Security, slide 15; 052 - Web Security, slide 16

PART A - QUESTION 8

A8a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State the two stages of the biometric authentication process and, for each stage, name the activities it involves.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identification stage: acquisition, creation of master characteristics, and storage of master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	1.00

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Authentication stage: acquisition(s), comparison, and decision.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::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: 072 - Biometrics and Authentication, slide 5

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

Question:

Explain the categories of biometric applications and the characteristics of the biometric technologies used for authentication, giving examples of each category and the practical issues associated with these technologies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Biometric applications are divided into two sectors, namely 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)	0.57
2	The physiological 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)	0.67
3	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
4	A biometric is defined as a physiological or behavioural characteristic that can distinguish one person from another.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.88
5	Iris scanning requires no touch and overcomes the issues of retinal scanners.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.25 LOW
6	Fingerprint biometrics suffer from disadvantages such as racial issues, dirt, grime and wounds, and can be spoofed so liveness is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::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 7

PART A - QUESTION 9**A9a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

State two ways in which an intrusion detection system contributes to detecting and defending against attacks on a system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can confirm whether an attack succeeded or failed by examining the log entries recorded by a host-based IDS.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported	0.23 LOW
2	An IDS can provide detection and response to an attack in near real time.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported (stem gate)	0.56

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

Citations: 062 - Intrusion Detection System, slide 14

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

State six points that distinguish the three security concepts of vulnerability, threat and attack, and give one countermeasure example for a threat class, drawing on the course material.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A vulnerability is defined as a weakness of a system that can be exploited to damage assets.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.88
2	A threat is described as a potential violation of security rather than an actual one.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.57
3	An attack is the actual violation of security, distinguishing it from a mere threat.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.57
4	A threat is an object, person or other entity that represents a constant danger to an asset.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	1.00
5	An attack is a deliberate act that exploits a vulnerability.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	1.00
6	Sandboxing is a countermeasure providing a safe, protected and isolated environment to run or open suspected insecure programs or files.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 26 061 - Network Security::s26::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: 011 - Introduction to Computer Security, slide 28; 011 - Introduction to Computer Security, slide 9; 061 - Network Security, slide 26

PART A - QUESTION 10

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

Question:

Explain how a buffer overflow arises in a program such as the one using strcpy() into a fixed-size local buffer, and state what an attacker can achieve by exploiting it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The overflow occurs because strcpy() copies the input string without checking its length against the size of the destination buffer.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.29 LOW
2	By controlling the overflowing buffer content, the attacker can overwrite the saved return address and thereby hijack the program's execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.67

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

Citations: 051 - Software Security, slide 21; 051 - Software Security, slide 23

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

Question:

Windows is often described as offering rich but complicated protection facilities. Explain six aspects of Windows security mechanisms, covering how subjects and their credentials are handled, how resources and policies are organised, and why the complexity of these mechanisms can itself become a security problem.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify the active entities in Windows as processes and threads.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.60
2	State where the security credentials of a subject are kept.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.60
3	Describe the directory service introduced in Windows 2000 that organises users, groups, credentials, resources and policies.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.55
4	Name the hierarchical database holding critical system information such as the SAM database and security logs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 4 041 - Windows Security::s04::1	supported (stem gate)	0.50
5	Note that discretionary access control allows fine-grained control over many different kinds of entities, both in Windows and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.43 LOW
6	Explain that the very complexity of Windows security can backfire, since bad configuration or coding bugs can cause serious security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.36 LOW

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

Citations: 041 - Windows Security, slide 11; 041 - Windows Security, slide 21; 041 - Windows Security, slide 4; 041 - Windows Security, slide 6

PART B - QUESTION 1**B1a - 5 marks - supported by lecture slides (not lecturer-marked)****Scenario:**

A small company runs a shared Linux server where staff log in with user names and passwords. After several accounts were guessed by an attacker, the administrator is asked to strengthen how passwords are protected and managed on the system.

Question:

Explain five password security controls that the administrator can apply to protect the accounts on this server, and state how passwords should be stored.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control to the password files so that they cannot be read freely.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported	0.44 LOW
2	De-activate an account 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)	0.86
3	Display the time of the last login so users can notice unexpected access.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.44 LOW
4	Enforce password policies, for example for the root password.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.60
5	Store the password in encrypted form using a one-way hash function.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication::s08::1	supported (stem gate)	1.00

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: 022 - Identification and Authentication, slide 12; 022 - Identification and Authentication, slide 8

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

Discuss how single sign-on and Kerberos could reduce the password burden on the staff of the company in the scenario, and explain the design criteria that make Kerberos suitable for authenticating users across its distributed servers.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the number of passwords users must remember.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.25 LOW
2	Single sign-on reduces the effort needed to maintain 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	Kerberos is a client-server single sign-on architecture that automates authentication in large distributed environments.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 24 022 - Identification and Authentication::s24::1	supported (stem gate)	0.73
4	Kerberos is designed so that passwords are never sent over the network in clear text, protecting against eavesdropping.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported	0.42 LOW
5	Kerberos is transparent, so after the initial login the user is unaware of further authentication.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.56

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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 24

PART B - QUESTION 2

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

Scenario:

A hospital wants to prove to auditors that every server booted only approved software. The vendor proposes placing a tamper-resistant chip on each motherboard and building a chain of trust from that chip upward through the boot software.

Question:

Referring to the hospital's proposed tamper-resistant chip, explain how a chain of trust is established from the hardware up to the running platform, and state what the chip is responsible for.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The chain of trust begins at the hardware TPM and then proceeds through the software stages (RTM, TPM software stack, BIOS, kernel).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.36 LOW
2	At each stage, the current stage measures and validates the next one.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.80
3	The resulting measurements are recorded in Platform Configuration Registers (PCRs) on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.75

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The TPM is a tamper-resistant hardware module mounted in the platform.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 6 073 - Trusted Computing::s06::1	supported (stem gate)	1.00
5	The TPM is responsible for 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)	0.89

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:

The vendor's tamper-resistant chip is said to support NGSCB. State five things about the Nexus and the Nexus Computing Agent that the hospital's security team should understand before relying on this design.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is a security kernel that is authenticated when the platform boots.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.57
2	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
3	Nexus does not place trust in the operating system.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported	0.43 LOW
4	The Nexus Computing Agent is a trusted software component that runs in trusted mode and communicates with Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.62
5	Developers are able to create their own agents to run on the trusted platform.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.75

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.