



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 16 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: 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 - 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:

Describe substitution ciphers by explaining what operation they perform on plaintext, what serves as the key, which security principle they relate to, and how larger blocks and varying substitutions are used to overcome their weaknesses. Include six points.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that substitution ciphers work by replacing each plaintext letter with 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	Identify the substitution rule itself as the key of the cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.50
3	Relate substitution to Shannon's principle of confusion.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.60
4	Explain that using larger blocks of letters as the basis of substitution leads to block ciphers.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 11 031 - Classical Cryptography::s11::1	supported (stem gate)	0.71
5	Note that applying different substitutions removes frequency features and leads to polyalphabetic substitution ciphers.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 11 031 - Classical Cryptography::s11::1	partly supported	0.25 LOW
6	State that the Arabs broke monoalphabetic substitution by means of frequency analysis.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 10 031 - Classical Cryptography::s10::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 10; 031 - Classical Cryptography, slide 11; 031 - Classical Cryptography, slide 4

PART A - QUESTION 2

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

Question:

Explain how a chain of trust is established in the Trusted Computing architecture, including the role played by the TPM and the roots of trust.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The chain of trust is the central concept of the Trusted Computing architecture, in which each stage measures and validates the following stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.30 LOW
2	The measurements produced during this process are recorded in Platform Configuration Registers (PCRs) held on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.55

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

Citations: 073 - Trusted Computing, slide 8

A2b - 6 marks - supported by lecture slides (not lecturer-marked)**Question:**

Refer to your answer in (a). Explain six components and characteristics of the NGSCB/Nexus architecture, covering the Nexus kernel, the Nexus Computing Agent, and how these relate to the TPM and the platform's trusted mode.

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
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	Nexus does not trust the operating system.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.50
5	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
6	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.

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

PART A - QUESTION 3**A3a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List TWO (2) reasons why software is insecure, with particular reference to buffer overflows.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Attackers can modify system 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)	0.79
2	A key source of software insecurity is the failure to validate user input.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.86

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

Citations: 051 - Software Security, slide 30

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

Describe six (6) aspects of the security mechanisms found in Windows systems, covering the overall mechanism set, access control, subjects and credentials, access rights, directory services, and the risks arising from complexity.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides complex mechanisms covering user account management, object management and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.82
2	Discretionary access control in Windows allows fine-grained control over diverse entities both in the OS and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.50
3	In Windows, subjects are processes and threads, and their security credentials are kept in a token.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.50
4	Access rights in Windows are encoded as a 32-bit mask and include standard rights such as DELETE and WRITE_DAC.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 16 041 - Windows Security::s16::1	partly supported	0.25 LOW
5	Active Directory, introduced in Windows 2000, is an LDAP-like directory service that organizes users, groups, credentials, resources and security policies.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.67
6	The complexity of Windows security is a weakness because misconfiguration and implementation bugs can cause severe security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.58

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: 041 - Windows Security, slide 11; 041 - Windows Security, slide 16; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

PART A - QUESTION 4

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

Question:

State TWO (2) formal security models that are listed as key security models, and for each, state the specific security concern it addresses.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula (BLP) model is a key security model that deals with access control only.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.78
2	The Chinese Wall model is a key security model that addresses the identification of conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::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: 024 - Formal Security Model, slide 5

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

Question:

Explain the access control structures used to implement access policies, covering the access control matrix, access control lists and capabilities, and state the requirements such structures must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control structures are the mechanisms through which access policies are implemented, and the access control matrix, capabilities and access control lists are named as such structures.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.60
2	The access control matrix is 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
3	The access control matrix suffers from poor scalability and poor handling of changes.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.25 LOW
4	An access control list is an object-centered description of access rights, illustrated by entries such as a document listing which users may read or write it.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	partly supported	0.36 LOW
5	Access control lists give easy access to an object's access rights and are relatively easy to manage using abstractions, but they give a poor overview of rights per subject and make revocation and sharing difficult.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	partly supported	0.33 LOW
6	Access control structures must be able to express control policies, allow verification of correctness, and be scalable and manageable.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::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: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 7; 023 - Access Control and Authorization, slide 8

PART A - QUESTION 5

A5a - 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
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves by appearing to be useful or benign programs so users install them willingly.	[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 can steal private data, delete files, record keystrokes, or create a way for additional malware to be installed.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.50

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

Citations: 051 - Software Security, slide 12

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

Question:

Discuss six ways in which malware attacks and propagates through a computer system, referring to the techniques malware uses to spread, hide, and affect the infected host.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Malware can propagate by self-replication, with programs copying themselves to improve their chances of survival.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 6 051 - Software Security::s06::1	supported (stem gate)	0.55
2	A virus can spread through boot sector infection of distributed media, as demonstrated by early malware included in the boot sector of software diskettes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.40 LOW
3	A worm can propagate remotely by exploiting a debugging feature that allows remote execution, as the Morris worm did across the Arpanet.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.25 LOW
4	An executable virus can attach its body to a legitimate program so that the infected file carries the malicious code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported	0.25 LOW
5	A rootkit hides malicious processes and software so that the infected machine remains under the control of the malware author.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.50
6	Spyware steals user credentials and records activity such as keystrokes and visited sites, which can lead to identity theft.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.36 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 10; 051 - Software Security, slide 13; 051 - Software Security, slide 6; 051 - Software Security, slide 7

PART A - QUESTION 6

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

Question:

State TWO (2) impacts of a security attack on the confidentiality, integrity or availability of a system's assets.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An attack may cause disclosure, which is unauthorized access to information and harms confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported	0.44 LOW
2	An attack may cause disruption, which is interruption or prevention of correct operation and harms availability.	[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

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 10

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

Question:

Discuss the Samy worm as an example of a cross-site scripting (XSS) attack, covering how the malicious script was injected, how it spread between users, and the scale of the resulting infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by manipulating the document body content.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.60
2	It retrieved the victim's list of friends (heros) by issuing a GET request to a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.33 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 profile had their own profile and friends list infected, enabling self-propagation.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW
5	The infection ultimately reached approximately one million MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.29 LOW
6	The attack exploited the fact that any web application returning unfiltered user input is a potential XSS vulnerability.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.69

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 13; 052 - Web Security, slide 15

PART A - QUESTION 7

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

Question:

State 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
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct within a society.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.67
2	Laws are described as 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

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

Question:

The ACM Code of Ethics and Professional Conduct guides computing professionals. State SIX (6) obligations that the ACM code places on a computing professional in their conduct and ethical practice.

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
3	The professional must be aware of and respect the rules that apply to 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)	0.57
4	The professional must contribute to the well-being of society and recognise that everyone is a stakeholder 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)	0.56
5	The professional must be honest and trustworthy in their dealings.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.40 LOW
6	The professional must treat people fairly and avoid discriminatory actions.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::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: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12

PART A - QUESTION 8

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

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS detects malicious activity occurring in computer systems.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported (stem gate)	0.71
2	A passive detection system can only log and alert when an attack is identified, and cannot actively stop an attack that is in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::1	partly supported	0.46 LOW

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

Citations: 062 - Intrusion Detection System, slide 2; 062 - Intrusion Detection System, slide 29

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

State six (6) points about threat classes and the countermeasures used against them, covering how threats differ from vulnerabilities and attacks, how misuse-based detection recognises known attack patterns, and how preventive mechanisms such as firewalls, sandboxing and input sanitisation reduce the risk from malicious activity.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A threat is described as a potential violation of security, distinguishing it from an actual attack.	[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
2	An attack is the actual violation of security, as opposed to a mere vulnerability or 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)	0.50
3	Misuse detection represents attacks as patterns or signatures so that variations of the same attack can be recognised.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	supported (stem gate)	0.80
4	A firewall is a preventive countermeasure that 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)	0.67
5	Sandboxing counters threats by providing a safe, isolated environment in which suspected insecure programs or files can be run or opened.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 26 061 - Network Security::s26::1	supported (stem gate)	0.64
6	The security of web applications depends crucially on sanitising user input to counter attacks such as XSS and XSRF.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 22 052 - Web Security::s22::1	supported (stem gate)	0.61

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 9; 052 - Web Security, slide 22; 061 - Network Security, slide 26; 061 - Network Security, slide 3; 062 - Intrusion Detection System, slide 17

PART A - QUESTION 9

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

Question:

Explain where network-based IDS sensors should be placed in a network and why their placement matters.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors should be positioned at strategic points so that the most valuable assets are protected.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.56
2	Typical sensor locations include just inside the firewall, on the DMZ, on the server farm segment, and on segments connecting mainframe or midrange hosts.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	partly supported	0.20 LOW

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

Citations: 062 - Intrusion Detection System, slide 7

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

Question:

Explain six preventive network security mechanisms and services that an organization can deploy to protect its network, describing what each mechanism does and how it contributes to securing network access and communication.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Remote Access VPN gives individual hosts or clients secure access to the organization's network from remote locations.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.80
2	Zero Trust Network Access restricts each user to only the access and permissions needed for their role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.50
3	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
4	Preventive techniques such as firewalls, proxy servers, packet-filtering routers and network segmentation stop some intrusions, while IDS monitors for attacks that get past them.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 3 062 - Intrusion Detection System::s03::1	supported (stem gate)	0.67
5	Transport layer security (SSL/TLS) provides secure end-to-end communication over TCP that is not limited to HTTP.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 18 061 - Network Security::s18::1	supported (stem gate)	0.61
6	Application layer security such as SSH secures remote login and services over an insecure network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 22 061 - Network Security::s22::1	partly supported	0.46 LOW

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

Citations: 061 - Network Security, slide 18; 061 - Network Security, slide 22; 061 - Network Security, slide 4; 062 -

PART A - QUESTION 10**A10a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List the TWO (2) stages of the biometric authentication process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identification stage, in which master characteristics are acquired, created and stored	[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	Authentication stage, in which acquisition is repeated and followed by comparison and a decision	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::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: 072 - Biometrics and Authentication, slide 5

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

Compare the two categories of biometric applications available today by identifying the biometric technologies that belong to each category, and then discuss three disadvantages associated with fingerprint biometrics.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Biometric applications are divided into two sectors, namely psychological 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 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
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	Fingerprint biometrics suffer from racial issues.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Fingerprint readings are affected by dirt, grime and wounds.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.50
6	Fingerprint biometrics can be spoofed, so liveness detection is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.57

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: 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7

PART B - QUESTION 1

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

Question:

State the role of a reference monitor in authorization and outline the four goals of access control. Then state the specific concern that the Chinese Wall policy is designed to address and explain why its permissions change dynamically.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A 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
2	One goal of access control is granting 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)	1.00
3	Another goal is limiting 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)	0.50
4	The Chinese Wall policy is designed to address conflicts of interest by a consultant or contractor.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	1.00
5	Permissions change dynamically because access rights depend on the 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)	0.56

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

Citations: 023 - Access Control and Authorization, slide 4; 024 - Formal Security Model, slide 24; 024 - Formal Security Model, slide 27

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

Question:

Explain the Chinese Wall model by stating the conflict it is designed to resolve, its classification as a policy type, the condition under which a subject may be granted access to an object, and the two conditions that must hold before write access is permitted.

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	It is classified as an access control confidentiality policy rather than an integrity policy.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.62
3	Under the simple security rule, a subject may access an object only if that object lies within the same company datasets already accessed (within the Wall).	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	supported	0.38 LOW
4	Alternatively, access is allowed if the object belongs to a completely 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	0.44 LOW
5	Write access is allowed only when the simple security rule permits it and no readable object in a different company dataset holds unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 26

PART B - QUESTION 2

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

Question:

Discuss FIVE (5) password security controls that an administrator can apply to protect user accounts on a Linux system, and explain how each control reduces the risk of unauthorized access.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control to the password files so that ordinary users cannot read stored password data.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.36 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	De-activate an account after several failed login attempts to block repeated guessing.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.50
3	Show the time of the last login so a user can notice suspicious account use.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.33 LOW
4	Store passwords only in encrypted form using a one-way hash function rather than plaintext.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication::s08::1	supported (stem gate)	0.64
5	Enforce password expiration so that a compromised password causes damage only for a limited period.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 10 022 - Identification and Authentication::s10::1	supported	0.33 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: 022 - Identification and Authentication, slide 10; 022 - Identification and Authentication, slide 12; 022 - Identification and Authentication, slide 8

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

Question:

Explain the design criteria that Kerberos aims to satisfy and the benefits that single sign-on solutions such as Kerberos bring to large distributed environments.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Kerberos is designed to be secure against eavesdropping by never transmitting passwords in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.60
2	Kerberos is designed for reliability, since every use of a service requires prior authentication.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.67
3	Kerberos is designed for transparency, so the user is unaware of any authentication beyond the initial login.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.70

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Kerberos is designed for scalability, supporting a large number of servers and clients.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.75
5	Single sign-on methods such as Kerberos automate 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)	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 18; 022 - Identification and Authentication, slide 24

End of marking scheme.