



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: 0 slot(s). Supported theory: 24 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 x (2 + 6) = 80 marks. Part B: 2 x (5 + 5) = 20 marks. Total: 100 marks. Slots: 0 computed, 24 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:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojan horses disguise themselves by appearing to be 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	0.09 LOW
2	Once running, a Trojan can steal private data, delete files, capture keystrokes, or open 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)	0.56

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

Citations: 051 - Software Security, slide 12

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

Question:

Explain six techniques by which malware propagates itself or attaches its code to a host program, and describe the effect each technique has on the infected system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can spread through boot sector infection, as shown by 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	partly supported	0.46 LOW
2	A worm can propagate across a network by exploiting a remote execution feature of a service, as Morris worm used a debugging feature of sendmail.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.33 LOW
3	An executable COM infection appends the virus body to a program and replaces the program entry point with a jump to the virus body.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.64
4	After the virus code runs in a COM infection, it restores the original entry point and jumps to it so the host program still executes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.60

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	An executable EXE infection overwrites the program header to switch the entry point to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.60
6	In an EXE infection the virus jumps to the original entry point during execution so the infected program continues to run.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software 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: 051 - Software Security, slide 10; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART A - QUESTION 2

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

Question:

State TWO (2) differences between morals and laws as forms of conduct guidance for computing professionals.

Marking points:

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 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

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

Question:

Describe six (6) professional conduct obligations that the ACM code places on a computing professional, and explain why such a documented code is needed to guide conduct in the computing profession.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional must work to a high standard of quality in the processes and products of 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 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	The professional must be aware of, and comply with, the rules that apply to professional work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported	0.43 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The professional must give and receive suitable professional review of work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported	0.33 LOW
5	The professional must contribute to society and human well-being, recognising all people as 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 documented code is needed because it sets out a written record of the behaviours that are acceptable for a professional group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.42 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; 071 - Ethics and Computer Security, slide 6

PART A - QUESTION 3

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

Question:

Explain the two stages of the biometric authentication process and state what happens during each stage.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage involves acquiring the biometric sample, creating the master characteristics and storing them.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.30 LOW
2	The authentication stage involves further acquisition(s), comparison against the stored data 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)	0.50

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:

State six facts about biometric mechanisms and technologies as presented in the course, covering the definition of a biometric, the two application sectors, the behavioural examples, the physiological examples, the fingerprint process, and the iris scanning advantages.

Marking points:

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

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 available today are divided into two sectors.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.86
3	The behavioural category of biometrics 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)	0.57
4	The physiological category of biometrics 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)	0.60
5	In fingerprint processing, the print is divided into loops, whorls and arch, and minutiae points such as ridge endings are calculated.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 6 072 - Biometrics and Authentication::s06::1	partly supported	0.43 LOW
6	Iris scanning requires no touch and overcomes the issues associated with retinal scanners.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.22 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: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 6

PART A - QUESTION 4

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

Question:

State TWO (2) classes of threat and, for each, the type of harm it causes to a system's assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class in which information is accessed without authorisation, harming confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported	0.33 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Deception is a threat class in which false data is accepted, harming 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

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

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

Question:

The Samy worm spread through MySpace by exploiting a cross-site scripting flaw. Explain how this worm injected its payload, how it harvested and recruited each victim's friends, 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 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 victim'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	It added Samy as a field by performing XML-HTTP requests against 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 with the JavaScript.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.67
5	The infection eventually reached roughly one million MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.43 LOW
6	The underlying flaw is that any web application returning user input without filtering 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)	0.77

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

Citations: 052 - Web Security, slide 13; 052 - Web Security, slide 15

PART A - QUESTION 5

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

Question:

Explain two ethical impacts that technology can have on society, and describe how a professional code of ethics helps computing professionals respond to such impacts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Technology can affect society by raising questions about acceptable standards of behaviour, which a code of ethics helps to clarify.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	partly supported	0.14 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Technology impacts everyone, so a code communicates shared guidelines that all professionals can follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	partly supported	0.36 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 8

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

Question:

Refer to your answer in (a). Based on the scenario in (a), discuss how the computing professional's responsibility for privacy should be exercised, referring to the ACM code of ethics and professional conduct and to the responsibilities of information specialists working within ethical, moral, and legal constraints.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional should recognise that the ACM is a professional body that maintains a code of ethics and professional conduct to guide members.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.46 LOW
2	The professional should acknowledge that merely describing the moral and ethical dimensions of ICT is insufficient when handling private data.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.39 LOW
3	The professional should accept that users in general, and information specialists in particular, have definite responsibilities for performing within ethical, moral, and legal constraints.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.82
4	The professional should be aware that other bodies such as AITP provide quality IT-related education and forums for networking with experienced peers, supporting responsible conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.56
5	The professional should recognise that the IEEE Computer Society is another professional body whose code can guide conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.23 LOW
6	Information specialists must carry out their duties within ethical, moral, and legal constraints, which is a definite responsibility.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.69

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 6

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

Question:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall model is designed to address conflicts of interest affecting 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)	0.80
2	Access decisions in the Chinese Wall model 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 24 024 - Formal Security Model::s24::1	supported	0.42 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 24; 024 - Formal Security Model, slide 27

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

Compare the access control matrix, access control lists and capability lists as structures for implementing access policies, and explain the requirements that any such access control structure must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control structures are mechanisms used to implement access policies, and the matrix, capability lists and ACLs are named examples of 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)	0.55
2	The access control matrix is one of the listed structures for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.50
3	Capability lists (C-List) are one of the listed structures for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.20 LOW
4	Access control lists (ACL) are one of the listed structures for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.50
5	A required property of an access control structure is the ability to express control policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Further requirements are verifiability of correctness together with scalability and manageability.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	partly supported	0.14 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 7

PART A - QUESTION 7

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

Question:

Explain the goals that access control pursues and the role of a reference monitor in realizing access control policies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control has four goals: granting, limiting, preventing and revoking 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)	0.88
2	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

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

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

Question:

State six points about the formal security models covered in the lecture, covering the BLP and Biba models, the Chinese Wall model, and the classification of the Chinese Wall policy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The BLP model is described as providing 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)	0.83
2	The Biba model is described as adding integrity verification on top of access control.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The Chinese Wall model is characterized by 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)	0.86
4	The Chinese Wall policy was proposed by Brewer and Nash in 1989 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
5	Strictly speaking, the Chinese Wall policy is 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)	0.64
6	Under the Chinese Wall simple security rule, a subject may access an object only if it lies within the Wall or belongs to an entirely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	partly supported	0.22 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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 5

PART A - QUESTION 8

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

Question:

State TWO (2) facts about the chain of trust in trusted computing, including how measurements are recorded and where the chain begins.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the chain measures and validates the following stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.60
2	The measurements are stored 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)	0.86

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Explain the roles of the two primary system components of the Next Generation Secure Computing Base (NGSCB), describing what each component does and how they relate to the trusted platform.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is a special kernel that forms the core of the trusted operating environment.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.62

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Nexus isolates normal-mode processes from trusted-mode processes by placing them differently in memory.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.67
3	Nexus authenticates and protects data that is entered, stored, communicated, and displayed by encrypting it.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.89
4	Nexus acts as 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
5	Nexus is a security kernel that is authenticated on boot and authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.57
6	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

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

Citations: 073 - Trusted Computing, slide 13; 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 9

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

Question:

List TWO (2) key 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 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)	0.72
2	A major 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)	0.75

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

Citations: 051 - Software Security, slide 30

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

Question:

Discuss six (6) aspects of Windows security mechanisms, covering the purpose of its access control facilities, the role of Active Directory and tokens, the historical security milestones, and the risks that arise from the complexity of these mechanisms.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides sophisticated mechanisms for managing user accounts, objects and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.80

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Discretionary access control in Windows allows fine-grained control over diverse entities 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)	0.55
3	The very complexity of Windows security can backfire, since misconfiguration and implementation bugs can cause serious incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.46 LOW
4	Active Directory, introduced with Windows 2000, is an LDAP-like directory service used to organise system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.91
5	Security credentials for a Windows subject are held in a token, which maps principals to subjects and carries extra security attributes.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	partly supported	0.36 LOW
6	Windows Vista (2007) marked a security milestone by removing admin-by-default and adding a firewall and DEP.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 2 041 - Windows Security::s02::1	supported	0.42 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: 041 - Windows Security, slide 11; 041 - Windows Security, slide 2; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

PART A - QUESTION 10

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

Question:

List two ways in which an intrusion detection system can help defend a system against attacks, according to the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can verify whether an attack succeeded or failed by reviewing HIDS log entries.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported (stem gate)	0.55
2	An IDS can provide near real-time detection and response to attacks.	[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.

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

Citations: 062 - Intrusion Detection System, slide 14

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

Question:

Describe three classes of threat to a computer system and, for each class, state one countermeasure that the lecture associates with preventing, detecting or recovering from it.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A threat is defined as an entity that represents a constant danger to an asset, i.e. a potential violation of security rather than an actual one.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	partly supported	0.46 LOW
2	A threat is only a potential violation of security, whereas an attack is the actual violation, so the two classes must be distinguished.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	partly supported	0.36 LOW
3	Software threats form a class that includes modification of program code and self-replicating code such as viruses.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	supported	0.42 LOW
4	Malicious software such as spyware is a threat class that steals user logins and passwords and can lead to identity theft.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	partly supported	0.29 LOW
5	A countermeasure for the threat of vulnerable software is prevention through vulnerability scanning and software updates.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 19 011 - Introduction to Computer Security::s19::1	supported (stem gate)	0.62
6	Detection countermeasures against threats include antivirus programs and intrusion detection systems.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 19 011 - Introduction to Computer Security::s19::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: 011 - Introduction to Computer Security, slide 19; 011 - Introduction to Computer Security, slide 28; 011 - Introduction to Computer Security, slide 9; 051 - Software Security, slide 13; 051 - Software Security, slide 2

PART B - QUESTION 1

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

Scenario:

A system administrator is reviewing how a shared UNIX server protects its user accounts. She wants to strengthen the controls applied to the stored password files and to the way accounts behave after repeated failed logins, while keeping the login process usable for staff.

Question:

Discuss FIVE (5) password security controls that can be applied to protect user accounts on a shared system, as presented in the course.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The system should display the time of the last login to the user.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.57
4	Password policies should be defined, 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)	0.50
5	Passwords should be stored in an 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)	0.88

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:

The administrator in the scenario is considering single sign-on for the shared UNIX server. Explain how Kerberos and related single sign-on mechanisms address authentication in such an environment, giving FIVE (5) points as presented in the course.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden of remembering passwords for users.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.29 LOW
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	Kerberos is a single sign-on method that automates authentication across 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)	0.90
4	Kerberos is designed to resist eavesdropping by never sending passwords in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported	0.44 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Kerberos is transparent, 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)	0.78

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: 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)

Question:

Explain the architecture of a Network-Based Intrusion Detection System by describing how sensors should be placed and what strengths this architecture offers the campus network team.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors must be positioned deliberately so that the most valuable assets are defended.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.62
2	A typical sensor location is 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
3	Because the IDS is shared, the overall cost of ownership is lower.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 8 062 - Intrusion Detection System::s08::1	supported (stem gate)	0.57
4	The sensor can examine all network traffic through packet analysis.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 8 062 - Intrusion Detection System::s08::1	supported	0.44 LOW
5	Captured packets are stored on a separate machine, which supports evidence preservation.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 8 062 - Intrusion Detection System::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: 062 - Intrusion Detection System, slide 7; 062 - Intrusion Detection System, slide 8

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

Question:

State five preventive network security mechanisms that a campus network team could deploy, giving for each the specific protective role it plays in controlling or securing network traffic.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall screens traffic entering and leaving the network according to rules set in advance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported	0.20 LOW
2	A proxy server improves both data protection and network throughput while also filtering web content.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported	0.46 LOW
3	Network segmentation draws boundaries so that assets sharing a function, risk or role sit inside the same segment.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.58
4	A remote access VPN lets individual hosts or clients reach the organization network securely from outside.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.67
5	Zero Trust Network Access restricts each user to only the access and permissions their role actually needs.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::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: 061 - Network Security, slide 3; 061 - Network Security, slide 4

End of marking scheme.