



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: $10 \times (2 + 6) = 80$ marks. Part B: $2 \times (5 + 5) = 20$ 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:

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
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

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

Question:

Describe six (6) professional conduct requirements that the ACM code of ethics places on a computing professional, as presented in the lecture on ethics and computer security.

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 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The professional must be aware of, and respect, the existing 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 (stem gate)	0.62
4	The professional must give and accept suitable professional review.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.60
5	The professional must only carry out work in areas where they are competent.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported	0.40 LOW
6	The professional must design and implement systems that are both robustly and usably secure.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.67

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 12

PART A - QUESTION 2

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

Question:

A company is deploying a network-based intrusion detection system (NIDS) across its campus network. List TWO (2) typical locations where NIDS sensors should be placed.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors should be positioned on the network segment just inside the firewall.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.38 LOW
2	Sensors should be positioned on the demilitarized zone (DMZ).	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.17 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

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

Question:

Explain three preventive network security mechanisms that an organization can deploy to protect its network, and for each mechanism describe how it controls or secures network traffic.

Marking points:

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

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 acts as a firewall and web filter, provides shared network connections, and caches data to speed up common requests, improving data security and network performance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.83
3	Network segmentation creates boundaries between network segments whose computing assets share a common function, risk, or role within the organization.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
4	A remote access VPN provides individual hosts or clients with remote and secure access to an organization's network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.90
5	Zero Trust Network Access (ZTNA) ensures a user only has the access and permission required to fulfill the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.61
6	Intrusion detection/prevention systems detect or prevent network security attacks such as brute force attacks, Denial-of-Service attacks, 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)	0.86

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 3

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

Question:

Explain the Chinese Wall model as a formal security model, stating the specific concern it was 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 policy was proposed by Brewer and Nash to address conflicts of interest, and it 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)	0.57
2	Access decisions under the Chinese Wall depend on the subject's history of past accesses, so permissions change dynamically rather than being fixed in advance.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported	0.31 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 24

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

Question:

Describe six points about the access control matrix, access control lists and capabilities as access control structures, covering what each structure represents and the stated advantages or disadvantages of these structures.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is presented as a basic control structure for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.43 LOW
2	The matrix is credited with clarity of definition and being easy to verify.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported (stem gate)	0.50
3	The 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	supported (stem gate)	0.50
4	An ACL is described as an object-centred description of access rights.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.83
5	ACLs give easy access to object access rights and are relatively easy to manage using abstractions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.88
6	ACLs are disadvantaged by a poor overview of access rights per subject and by difficulty of revocation and sharing.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.73

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 8

PART A - QUESTION 4**A4a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List TWO (2) facts about the chain of trust in Trusted Computing, including how measurements are stored and where the chain begins.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Measurements taken during the chain of trust are recorded in Platform Configuration Registers (PCRs) located on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The chain of trust originates at the hardware TPM and then proceeds through software components such as RTM, TPM Software Stack, BIOS and kernel.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.64

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 8

A4b - 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), and describe how the Nexus interacts with trusted software and the TPM.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The 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
2	The 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	The 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
4	The Nexus provides the application interface to the TPM and does not trust the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.38 LOW
5	The Nexus Computing Agent (NCA) is a trusted software component that runs in trusted mode and communicates with the Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.56
6	NCA specifications are open-source, allowing developers 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)	0.55

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 5

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

Question:

State TWO (2) ways in which a documented code of ethics guides the ethical conduct of computing professionals, 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	It makes the accepted standards of behaviour clearer to understand.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported (stem gate)	0.50
2	It communicates shared guidelines that everyone is expected to follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::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: 071 - Ethics and Computer Security, slide 8

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

Question:

Compare the responsibilities that the ACM code of ethics places on a computing professional with respect to privacy and confidentiality, and explain how a documented code of ethics supports an organisation in enforcing acceptable professional behaviour.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional must protect personal information by respecting privacy as a stated obligation.	[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
2	The professional must safeguard information entrusted to them by honouring confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.12 LOW
3	The professional must act honestly and be worthy of trust when handling stakeholder data.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.10 LOW
4	The professional must consider all people affected by computing as stakeholders and contribute to their well-being.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.60
5	A code of ethics is a written record of the behaviours a professional group deems acceptable.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.33 LOW
6	The code is established by the professional body itself, giving the organisation authority to define what counts as appropriate conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	partly supported	0.09 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 6

PART A - QUESTION 6**A6a - 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 those master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.33 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

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

Refer to your answer in (a). A bank plans to replace password logins at its branch counters with biometric authentication. Explain six points the bank must consider regarding biometric mechanisms and technologies, covering the definition of a biometric, its categories, and specific technologies with their limitations.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A biometric is defined as a physiological or behavioural characteristic of a human being that can distinguish one person from another and can theoretically be used for identification or verification of identity.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.92
2	Biometric applications are categorized into two sectors, namely psychological (physiological) and behavioural.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.62
3	The psychological category includes iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.78
4	The behavioural category includes voice, typing pattern and signature.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.67

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Iris scanning reads the unique pattern of the iris, requires no touch, and overcomes retinal scanner issues, though contact lenses may be an issue.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.27 LOW
6	Fingerprint biometrics suffer disadvantages such as racial issues, dirt, grime and wounds, finger placement problems, and the need for liveness detection because they can be spoofed.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.15 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 7

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

Question:

State TWO (2) characteristics of a Trojan horse as a type of malware.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans typically disguise themselves as useful or benign programs.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.17 LOW
2	Trojans steal private information or otherwise damage the host system.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.25 LOW

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

Citations: 051 - Software Security, slide 12

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

Question:

Explain six (6) techniques by which malware propagates itself or infects host programs and systems, as described in the lecture material.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can spread by infecting the boot sector of a disk.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.57
2	A worm can propagate across a network by exploiting a remote execution feature of a service such as sendmail.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported	0.27 LOW
3	An executable COM file can be infected by appending the virus body to the program and redirecting the entry point to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	partly supported	0.33 LOW
4	An executable EXE file can be infected by overwriting the program header so that the entry point switches to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	A rootkit is typically installed after a vulnerability has been found and detected, allowing the attacker to keep control of the infected machine.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.57
6	Spyware can redirect the user's browser to unwanted sites as part of its spying behaviour.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.50

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

Citations: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART A - QUESTION 8

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

Question:

Explain how the classes of threats described in the lecture can impact the confidentiality, integrity and availability of a system's assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure threats such as snooping, sniffing and wiretapping give 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	0.36 LOW
2	Deception involves acceptance of false data, and integrity services are the countermeasure against it.	[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.

Citations: 011 - Introduction to Computer Security, slide 10

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

Question:

Discuss the Samy worm as a case study of a cross-site scripting (XSS) attack, covering how the malicious script was injected, how it spread to other users, and the outcome of the incident.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by writing to the document body.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.67
2	The script retrieved the victim's list of friends (heros) 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	0.30 LOW
3	The worm 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, enabling self-propagation.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	The incident ultimately infected 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 root cause is 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)	0.75

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

PART A - QUESTION 9

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

Question:

Explain the goals of access control 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 aims to grant, limit, prevent and revoke access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.86
2	Reference monitors are the instruments used to realize access control policies and can be deployed at all levels of the system hierarchy.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	0.54

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 18; 023 - Access Control and Authorization, slide 4

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

Question:

Discuss the formal security models covered in the lecture, focusing on the Bell-La Padula, Biba and Chinese Wall models. In your answer, explain the concern each model addresses and the specific access rules that the Chinese Wall model imposes on subjects.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula model is presented as a formal model concerned 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)	0.75
2	The Biba model is distinguished from BLP by adding integrity verification.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.57

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The Chinese Wall model is described as identifying 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)	1.00
4	The Chinese Wall simple security rule permits a subject to access an object only when that object is either in the same company dataset as objects the subject has already accessed (i.e., within the Wall) or 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 (stem gate)	0.52
5	Under the Chinese Wall *-property, a write is allowed only if the simple security rule permits it and no readable object lies in a different company dataset while holding unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	supported (stem gate)	0.55
6	The Chinese Wall policy is designed to address the specific concern of conflicts of interest for a consultant or contractor, and its access decisions depend on the history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	0.67

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 25; 024 - Formal Security Model, slide 26; 024 - Formal Security Model, slide 27; 024 - Formal Security Model, slide 5

PART A - QUESTION 10

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

Question:

Explain two ways in which an intrusion detection system supports the detection and defence of a system against attacks.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can detect 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)	0.62
2	An IDS can identify and stop an attack that is currently in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::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: 062 - Intrusion Detection System, slide 2

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

Question:

State six (6) points from the lecture that characterise threat classes and the countermeasures used against them, covering how threats, attacks and vulnerabilities are distinguished, how malware is described, and how protective mechanisms are classified.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A threat is defined as 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)	0.90
2	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
3	Protection of assets covers prevention, detection and response techniques.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	0.86
4	A threat is characterised as a potential violation of security, whereas an attack is the actual violation.	[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
5	Malware research includes Cohen's formal definition of a virus and a mathematical description of how viruses propagate.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 6 051 - Software Security::s06::1	partly supported	0.40 LOW
6	Sandboxing is a countermeasure that provides a safe, protected and isolated environment for running or opening 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)	0.77

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; 051 - Software Security, slide 6; 061 - Network Security, slide 26

PART B - QUESTION 1

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

Scenario:

A small company runs a shared Linux server for its staff. The administrator notices that several users still rely on weak passwords and that failed login attempts are never acted upon. She decides to strengthen the password security controls on the server.

Question:

Explain five password security controls the administrator can apply to strengthen authentication on the shared Linux server.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control to the password files so that they are protected from unauthorised reading.	[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 user accounts automatically after several 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)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Show the time of the user's last login so that suspicious activity can be noticed.	[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	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 passwords in an encrypted form using a one-way hash function rather than in plain text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication:: s08::1	supported (stem gate)	0.64

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 wants to reduce the number of passwords staff must remember and type on the shared Linux server. Explain five points about single sign-on and Kerberos that she should understand before adopting such a mechanism.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden of remembering many passwords for users.	[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 cuts down 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	0.25 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 so that passwords are never transmitted 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 (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Kerberos is transparent to the user, who 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

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:

Discuss software insecurity and buffer overflows in the context of the consultant's review. Your answer should address the root causes of software insecurity, how a stack buffer overflow occurs, and the mitigation techniques available.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Explain that software insecurity arises because an attacker 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	Identify failed validation of user input as one of the key sources of software insecurity.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	1.00
3	Describe how a local buffer allocated on the stack can, without proper bound checking, overspill into the adjacent upper stack area.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.86
4	Explain that by controlling the buffer content an attacker can overwrite the return address with an arbitrary value and thereby hijack the execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.86
5	Name the special techniques for strengthening software security, namely canaries, address space layout randomization and data execution prevention.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::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: 051 - Software Security, slide 21; 051 - Software Security, slide 30

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

Question:

State five Windows security mechanisms or features that the consultant would examine, and for each, note the security concern it raises.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides complex mechanisms for managing user accounts and objects as well as controlling access.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.91

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Discretionary access control enables detailed control over access to diverse entities within Windows and its 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 these mechanisms can cause serious security incidents through misconfiguration or implementation bugs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.50
4	Active Directory, introduced with Windows 2000, acts as a directory service for organising system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.80
5	Security credentials for a subject are held in a token that maps principals to subjects and may carry 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

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 21; 041 - Windows Security, slide 6

End of marking scheme.