



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:

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 disguise themselves as useful or benign software in order to get executed.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Once running, a Trojan steals private data, deletes files, records keystrokes, or opens a way for additional malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.57

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:

State SIX (6) techniques by which malware propagates or conceals itself within an infected system, as described in the lecture on software security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can append its body to a host program and save the program's entry point inside the virus body.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.70
2	A virus can replace the program's entry point with a jump into the virus body, then restore and jump to the original entry point after executing.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.79
3	A virus can overwrite a program header so that the entry point switches to the virus, jumping back to the original entry point during execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.77
4	A rootkit hides malicious processes and software so that the infected machine stays under the malware author's control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	A rootkit is typically installed after a vulnerability has been found, and its detection is difficult because it is designed to stay hidden from detection software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.86
6	Spyware steals user logins and passwords, records visited sites, logs keystrokes and redirects browsers to unwanted sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.85

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

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

PART A - QUESTION 2

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

Question:

Explain the difference between morals, ethics and laws as three distinct forms of guidance for professional conduct.

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	Ethics is characterised as a set of guiding beliefs, standards or ideals held by an individual, group or community.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.73

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:

Discuss how a professional code of ethics and conduct guides a computer security practitioner, referring to the ACM code and the professional conduct expected of computing professionals. Support your discussion with six distinct requirements.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that a code of ethics is a documented set of acceptable behaviours defined by a professional or social group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.60
2	Identify the ACM as a professional body that has established a code of ethics and professional 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)	0.75
3	Explain that the code obliges the professional to respect privacy.	[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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Explain that the code obliges the professional to honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.20 LOW
5	Describe the duty to keep up high standards of professional 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
6	Describe the duty to design and build systems that are 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)	0.71

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

Citations: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12; 071 - Ethics and Computer Security, slide 6; 071 - Ethics and Computer Security, slide 7

PART A - QUESTION 3

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

Question:

State TWO (2) ethical responsibilities that information specialists carry when working with ICT, according to the discussion of moral and ethical dimensions.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Information specialists are expected to perform their duties 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)	0.60
2	Merely describing the moral and ethical dimensions of ICT is insufficient; the ethical impacts must be actively addressed.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.40 LOW

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

Citations: 071 - Ethics and Computer Security, slide 3

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

Question:

Explain six (6) points about how an organisation's ethical code shapes professional conduct and responsibility, including what the code adds, how it guides staff, and what consequences may follow when it is not followed.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An organisational ethical code adds clarity to the understanding of acceptable standards of behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported (stem gate)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The code communicates common guidelines that everyone in the organisation 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)	0.62
3	The organisation must consider what happens when a member does not follow its ethical code.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.36 LOW
4	For the ACM, adherence to the code is voluntary rather than enforced.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.29 LOW
5	For the Malaysian Bar Council, failing to follow the code can lead to revocation of the licence.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.30 LOW
6	A person separated from law and justice is described as the worst of all animals, showing why ethical and legal constraints matter.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	supported	0.42 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 4; 071 - Ethics and Computer Security, slide 8

PART A - QUESTION 4

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

Question:

Explain how a chain of trust is established in the Trusted Computing architecture, referring to the role of 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 next stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.40 LOW
2	The measurements produced at each stage 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)	0.60

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Describe six components and characteristics of the Next Generation Secure Computing Base (NGSCB), focusing on the Nexus and the Nexus Computing Agent (NCA).

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Nexus is 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	The 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	The Nexus provides the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.60
4	The Nexus 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 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)	0.62
6	The 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 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 5

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

Question:

State TWO (2) rules that govern access under the Chinese Wall model.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Under the Chinese Wall simple security rule, a subject may be granted access to an object only if the object is within the same company datasets already accessed by that subject (i.e., within the Wall), or it 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)	0.55
2	Under the Chinese Wall *-property, a write is allowed only if the simple security rule permits it and no object readable by the subject belongs to a different company dataset that holds unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	partly supported	0.30 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 25; 024 - Formal Security Model, slide 26

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

Question:

Describe the access control matrix, the access control list and the capability list as access control structures, giving one advantage and one disadvantage of the access control matrix and of the access

control list, and stating what a capability list associates with each subject.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is identified 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	An advantage of the access control matrix is that its definition is clear.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.17 LOW
3	A disadvantage of the access control matrix is that it scales poorly.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.33 LOW
4	An access control list 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)	0.67
5	An advantage of the access control list is that object access rights are easy to reach.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.57
6	A disadvantage of the access control list is the difficulty of revocation.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported	0.20 LOW

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

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

Citations: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 8

PART A - QUESTION 6

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

Question:

List TWO (2) reasons why software is insecure, as discussed in the Software Security lecture.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Attackers can tamper with 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)	0.71
2	A major source of software insecurity is the failure to properly validate user input.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.67

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

Citations: 051 - Software Security, slide 30

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

Question:

Compare the security mechanisms available in Windows with those available in UNIX, focusing on the strengths and weaknesses of each. Provide six (6) distinct points of comparison.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides complex 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)	0.90
2	Windows discretionary access control (DACS) allows fine-grained control over diverse entities in both the OS and applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.54
3	The complexity of Windows security can itself be a vulnerability, as misconfiguration or 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	UNIX offers flexible security mechanisms whose effectiveness depends on careful administration.	[verbatim slide quote omitted in public build]	042 - Linux Security, slide 28 042 - Linux Security::s28::1	supported (stem gate)	0.50
5	UNIX lacks several key security features such as ACLs and security levels.	[verbatim slide quote omitted in public build]	042 - Linux Security, slide 28 042 - Linux Security::s28::1	supported (stem gate)	0.71
6	UNIX's open source implementation is a strength because flaws are found and fixed quickly.	[verbatim slide quote omitted in public build]	042 - Linux Security, slide 28 042 - Linux Security::s28::1	supported	0.40 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 21; 042 - Linux Security, slide 28

PART A - QUESTION 7

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

Question:

A company is deploying a Network-Based Intrusion Detection System (NIDS) to protect its critical servers. List TWO (2) typical locations where IDS sensors should be placed.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Placing a sensor 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)	0.60

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Placing a sensor on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.33 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

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

Question:

Discuss the preventive network security mechanisms that an organization can deploy to control and protect its network traffic, and explain how these mechanisms relate to intrusion detection. Support your discussion with six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Firewalls control 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	Proxy servers act as a firewall and web filter while also providing shared network connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.86
3	Network segmentation creates boundaries between segments whose computing assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.77
4	Remote access VPNs provide individual hosts or clients with remote and secure access to an organization 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 restricts a user to only 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)	0.64
6	IDS monitors network resources to detect intrusions and attacks that preventive techniques such as firewalls, proxy servers, packet-filtering routers and network segmentations failed to stop.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 3 062 - Intrusion Detection System::s03::1	supported (stem gate)	0.84

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; 062 - Intrusion Detection System, slide 3

PART A - QUESTION 8

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

Question:

Explain how the disclosure and disruption classes of threats each affect the confidentiality, integrity and availability of information assets.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is described as unauthorized access to information, which harms confidentiality, and confidentiality services are the countermeasure.	[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
2	Disruption means interrupting or preventing correct operation, and availability services are what counter this threat.	[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

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

Question:

Refer to your answer in (a). The Samy worm spread through MySpace by exploiting a cross-site scripting flaw. Explain six distinct steps or effects of this worm as described in the lecture, covering how it injected code, gathered data, added friends, propagated to visitors, and the scale of infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile using document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
2	It obtained the list of the user's heroes by performing a GET request on a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.43 LOW
3	It added Samy as a friend by performing XML-HTTP on the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.88
4	Any user visiting an infected user's page had their profile infected with JavaScript and their friends list infected with Samy.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.80
5	Eventually about 1,000,000 MySpace profiles were infected.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.83
6	The underlying XSS vulnerability exists because any web application that returns user input without filtering is a potential XSS vulnerability, allowing execution of arbitrary JavaScript in the user's browser.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.53

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 9

A9a - 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 computer systems.

Marking points:

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

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	An IDS can identify and stop attacks that are 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

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

Question:

State six distinct points from the lecture that characterise threat classes and the countermeasures used against them, covering how threats differ from vulnerabilities and attacks, how web attacks such as XSS and SQL injection operate, and how protection mechanisms such as sandboxing and input sanitisation respond to these threats.

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	In an XSS attack the attacker inserts a malicious string into the website's database through one of its forms.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 16 052 - Web Security::s16::1	supported (stem gate)	0.80
4	In an SQL injection attack a crafted password condition that is always true permits unauthorised access.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 19 052 - Web Security::s19::1	supported	0.46 LOW
5	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
6	The security of web applications depends crucially on sanitising user input as a defence against typical attacks.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 22 052 - Web Security::s22::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: 011 - Introduction to Computer Security, slide 9; 052 - Web Security, slide 16; 052 - Web Security, slide 19; 052 - Web Security, slide 22; 061 - Network Security, slide 26

PART A - QUESTION 10

A10a - 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

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

Question:

Explain six points about biometric mechanisms and technologies, covering how a biometric is defined, the categories of biometric applications, and the characteristics and drawbacks of specific biometric technologies.

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 available today 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)	0.67
3	The psychological 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)	0.70
4	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
5	Iris scanning reads the unique pattern of the iris, requires no touch, and thereby 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	0.31 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Fingerprint biometrics suffer disadvantages such as racial issues, dirt, grime and wounds, finger placement problems, an overly large database to process, 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	0.12 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 B - QUESTION 1

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

Scenario:

A hospital group runs a shared clinical information system. Doctors and nurses request access to patient records, and the system must decide which subjects may reach which objects and in what way, while an administrator worries about how access decisions are enforced and how the underlying access structures scale.

Question:

Explain the goals that access control pursues and the role of the reference monitor in making authorization decisions, and describe the access control structures used to implement policies together with the requirements they must satisfy.

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	The reference monitor is the component that makes authorization decisions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	1.00
3	Reference monitors are the instruments through which access control policies are realized and can be deployed at every level 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)	0.86
4	The access control structures for implementing policies are the access control matrix, capabilities and access control lists, plus intermediate controls such as groups and roles.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.83
5	Any access control structure must be able to express control policies, allow verification of correctness, and remain scalable and manageable.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.57

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; 023 - Access Control and Authorization, slide 7

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

Question:

Discuss how formal security models address the hospital group's need to control access to patient records, referring to the Chinese Wall model's treatment of conflicts of interest, its dynamic permissions, and the role of past access history, and explain how the BLP and Biba models differ in what they verify.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall model is a hybrid model proposed by Brewer and Nash that addresses conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.78
2	The Chinese Wall 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)	0.56
3	Under the simple access control policy, a subject may access information from any company as long as it has never accessed information from a different company in the same conflict class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.75
4	Permissions in the Chinese Wall model change dynamically, with access rights depending 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)	0.73
5	The BLP model provides access control only, whereas the Biba model adds integrity verification.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.73

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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 24; 024 - Formal Security Model, slide 5

PART B - QUESTION 2

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

Question:

State five password security controls that can be applied to protect a system's password files and accounts, as covered in the lecture on identification and authentication.

Marking points:

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

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 an account after multiple failed login attempts.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.86
3	Display the time of the user's last login so anomalies can be noticed.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.50
4	Enforce password policies, for example for the root password.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.60
5	Store the password in encrypted form using a one-way hash function.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication::s08::1	supported (stem gate)	1.00

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

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

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

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

Question:

A campus network wants users to log in once and reach many servers without retyping passwords. Explain five points about single sign-on and Kerberos that the network designers should consider, covering the motivation for single sign-on, the authentication categories involved, Kerberos design criteria, the initial user authentication exchange, and the limitations of Kerberos.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on is motivated by reducing the need to memorize passwords and the time spent typing them, as well as lowering password maintenance effort.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	partly supported	0.29 LOW
2	Authentication factors are categorized as something you know (passwords, passphrases, shared secrets), something you have (smart cards, security tokens), and something you are (biometrics and behavioural traits).	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 9 022 - Identification and Authentication::s09::1	partly supported	0.35 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Kerberos design criteria include security against eavesdropping with no clear-text password transmission, reliability through prior authentication for every service use, transparency to the user, and scalability to many servers and clients.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	partly supported	0.30 LOW
4	In Kerberos user authentication, the client sends its user ID and requested service to the authentication server, which checks the database and returns a ticket-generating ticket and session key encrypted to the client.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 20 022 - Identification and Authentication::s20::1	partly supported	0.47 LOW
5	Kerberos provides secure authentication over an insecure network and is a de-facto standard, but it is relatively complex to install and constitutes a single point of failure.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 23 022 - Identification and Authentication::s23::1	partly supported	0.18 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 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 20; 022 - Identification and Authentication, slide 23; 022 - Identification and Authentication, slide 9

End of marking scheme.