



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

COURSE	:	COMPUTER SECURITY
COURSE CODE	:	CSC662
EXAMINATION	:	OCTOBER 2026 (MOCK)
TIME	:	3 HOURS

MARKING SCHEME NOTES

1. This marking scheme accompanies the CSC662 mock paper (October 2026).
Computed answers show working; theory answers are supported by lecture slides (not lecturer-marked); verbatim quotes are omitted in this public build; slide citations are retained.
2. Supported theory marking points quote the lecture decks; any unresolved slot would remain a visible placeholder.
3. Part A = $10 \times (2 + 6)$; Part B = $2 \times (5 + 5)$; total = 100 marks.
4. Computed: 1 slot(s). Supported theory: 23 slots. Placeholders: 0.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of 16 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

Labels: computed / supported by lecture slides (not lecturer-marked) / placeholder. No official marking scheme exists for the real CSC662 papers; this is generated for the mock.

Entailment labels: supported = the private quote directly supports the point (or the point passed the stem-overlap gate); partly supported = partial/ambiguous support; not supported = no support. Quote text is omitted here; verdicts come from private verification.

Part A: $10 \times (2 + 6) = 80$ marks. Part B: $2 \times (5 + 5) = 20$ marks. Total: 100 marks. Slots: 1 computed, 23 supported by lecture slides, 0 placeholder.

Methods: computed answers use verified solvers. Theory answers are supported by lecture slides (not lecturer-marked). Each point carries a deck/slide citation and overlap score; verbatim quote text is omitted from this public build. Low overlap is flagged for human review.

PART A - QUESTION 1

A1a - 2 marks - computed - matches lecture slides 5-9 (Caesar shift 3 examples)

Question:

Using Caesar Cipher technique, decrypt the following ciphertext with a shift of 7 (replace each letter with the one 7 positions to the left).

KLCPJLYLABYULKHUKDPWLKVUL

Answer: DEVICERETURNEDANDWIPIEDONE

Working:

```

K (10) -7 mod 26 -> D
L (11) -7 mod 26 -> E
C ( 2) -7 mod 26 -> V
P (15) -7 mod 26 -> I
J ( 9) -7 mod 26 -> C
L (11) -7 mod 26 -> E
Y (24) -7 mod 26 -> R
L (11) -7 mod 26 -> E
A ( 0) -7 mod 26 -> T
B ( 1) -7 mod 26 -> U
Y (24) -7 mod 26 -> R
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
H ( 7) -7 mod 26 -> A
U (20) -7 mod 26 -> N
K (10) -7 mod 26 -> D
D ( 3) -7 mod 26 -> W
P (15) -7 mod 26 -> I
W (22) -7 mod 26 -> P
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
V (21) -7 mod 26 -> O
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E

```

Suggested marks: 1 mark for identifying the cipher/shift direction; 1 mark for the complete plaintext.

Confidence: computed - matches lecture slides 5-9 (Caesar shift 3 examples).

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

Question:

Explain substitution ciphers by describing how plain-text is transformed, what serves as the key, how the approach relates to Shannon's principle of confusion, and how this idea carries over to modern ciphers.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that substitution replaces plain-text letters with other letters.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	1.00
2	Note that the transformed text produced by the replacement is the cipher-text.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.33 LOW
3	Identify the substitution rule as the key of the cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.67
4	Relate substitution to Shannon's principle of confusion.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.60
5	Explain that the substitution idea is employed in modern ciphers.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.60
6	Contrast with Vigenere, which uses a keyword to select encrypting rows and resists simple frequency analysis.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 14 031 - Classical Cryptography::s14::1	partly 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: 031 - Classical Cryptography, slide 14; 031 - Classical Cryptography, slide 4

PART A - QUESTION 2

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

Question:

State TWO (2) typical locations where IDS sensors are placed in a network-based IDS architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be positioned just inside the firewall.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.50
2	A sensor can be positioned on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.25 LOW

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

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

Citations: 062 - Intrusion Detection System, slide 7

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

Describe six (6) preventive network security mechanisms that an organization can deploy to protect its network, explaining what each mechanism does.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing network traffic according to predetermined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
2	A proxy server improves data security and network performance by acting as a firewall and web filter, sharing 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)	0.79
3	Network segmentation creates boundaries between network segments whose computing assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.77
4	A remote access VPN gives individual hosts or clients remote and secure access to the organization network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access (ZTNA) grants a user only the access and permission required to fulfil the user's role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.58
6	Intrusion detection/prevention systems detect or prevent network 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)	0.85

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:**

State TWO (2) facts about the chain of trust in Trusted Computing, focusing on how it begins and how measurements are recorded.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The chain of trust begins at the hardware TPM and then proceeds through software stages 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)	0.60
2	Measurements taken during the chain 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)	0.60

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

Citations: 073 - Trusted Computing, slide 8

A3b - 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, describing what each component is and how it supports trusted execution on the platform.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is described as 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	Nexus aims to isolate 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)	0.60
3	Nexus provides functionality to authenticate and protect data that is entered, stored, communicated, and displayed by means of encryption.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.67
4	Nexus acts as a security kernel that is authenticated at boot time.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.57
5	Nexus authenticates trusted programs and provides the application interface to the TPM, without trusting the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.33 LOW
6	The Nexus Computing Agent is a trusted software component that runs in a trusted mode and communicates with Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	partly supported	0.25 LOW

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

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

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

List the TWO (2) stages that make up the biometric authentication process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage, in which master characteristics are acquired, created and stored.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.50
2	The authentication stage, in which acquisition is repeated, followed by comparison and a decision.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.71

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

Citations: 072 - Biometrics and Authentication, slide 5

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

State the definition of a biometric as given in the lecture, and state the TWO (2) sectors into which today's

biometric applications are categorised. Then name the THREE (3) biometric technologies listed under the behavioural sector.

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	The two sectors are the physiological sector and the behavioural sector.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	partly supported	0.33 LOW
3	The psychological sector covers 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 sector covers 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
5	Biometric methods are listed as an alternative user authentication mechanism alongside smart cards and two-factor authentication.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 24 022 - Identification and Authentication::s24::1	supported (stem gate)	0.90
6	An iris scan reads the unique pattern of the iris, which is coloured and visible from far, and requires no touch.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly 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: 022 - Identification and Authentication, slide 24; 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4

PART A - QUESTION 5

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

Question:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojan horses conceal their malicious purpose by presenting themselves as useful or benign software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Once running, a Trojan can steal private data, delete files, capture keystrokes, or create a way for additional malware to be installed.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.50

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

Citations: 051 - Software Security, slide 12

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

Question:

Discuss six ways in which malware attacks and propagates, covering how malicious code is attached to executables, how early viruses and worms spread, how rootkits and spyware operate on infected hosts, and how self-replication supports propagation.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Malware can be attached to an executable by appending the virus body to a program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.50
2	An executable can be infected by overwriting its 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)	0.60
3	Early malware such as Elk Cloner spread through boot sector infection.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.40 LOW
4	The Morris worm propagated across the Arpanet by exploiting a debugging feature of sendmail for remote execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.40 LOW
5	Rootkits hide malicious processes and software so that the infected machine stays under the malware author's remote control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.54
6	Spyware steals user logins and passwords, records visited sites and logs keystrokes to support identity theft.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.61

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

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

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

PART A - QUESTION 6

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

Question:

Explain the difference between morals, ethics and laws as three forms of guidance for conduct in computer security work.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct, forming the basis of social behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.55

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

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

Question:

Explain six requirements that a professional code of ethics and conduct, such as the ACM code, places on a computing professional's behaviour in security-related work.

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
3	The professional must be aware of and respect the rules that apply to their professional work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.57
4	The professional should 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
5	The professional should avoid causing harm through their work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.29 LOW
6	The professional should respect privacy and honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	partly supported	0.33 LOW

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

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

PART A - QUESTION 7

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

Question:

Explain the Chinese Wall model as a formal access-control policy, stating the specific concern it addresses and how its access decisions depend on a subject's access history.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy is designed to address a specific concern: conflicts of interest involving 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)	0.91
2	Access rights under the Chinese Wall change dynamically, since what a subject may access depends on the history of its past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.61

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

A7b - 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 state the requirements that any such access control structure must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is identified as one of the structures used to implement 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)	0.83
2	Capability lists (C-List) are named as a structure 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
3	Access control lists (ACL) are named as a structure 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
4	An access control structure must be able 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	0.43 LOW
5	An access control structure must support verifiability of correctness.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.14 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	An access control structure must provide scalability and manageability.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.29 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 8

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

Question:

Explain what a buffer overflow is and how it can be exploited to hijack a program's execution flow.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A buffer overflow arises because the copy routine does not verify the length of the input string, so a longer string than the buffer can hold overflows it.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.19 LOW
2	Because bounds are not checked, the overflowing buffer content spills into the adjacent higher stack area, letting the attacker overwrite the return address with an arbitrary value and divert execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	partly supported	0.41 LOW

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

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

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

Question:

State six Windows security mechanisms or components and, for each, briefly indicate the security function it performs.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Security Reference Monitor operating in kernel mode performs ACL verification.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	partly supported	0.44 LOW
2	The winlogon process in user mode handles user logon.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.67
3	The Local Security Authority verifies and changes passwords and manages access tokens and audit logs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.82
4	The Security Accounts Manager holds the accounts database and performs password encryption.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.75
5	User Account Control enforces limited user privileges.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	1.00

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Active Directory acts as an LDAP-like directory service for organising system resources such as users, groups and security policies.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::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: 041 - Windows Security, slide 3; 041 - Windows Security, slide 6

PART A - QUESTION 9

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

Question:

State two classes of threats to a computer system and, for each, identify the security objective whose violation represents the harm caused.

Marking points:

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

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

Citations: 011 - Introduction to Computer Security, slide 10

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

Question:

Describe the Samy worm as a case study of a cross-site scripting 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 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 user's friends (heros) by issuing a GET request to a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.38 LOW
3	It added Samy as a friend 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 visitor to an infected profile had their own profile and friends list infected, which is how the worm propagated.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.33 LOW
5	The incident ultimately infected about 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The underlying weakness is that any web application returning user input without filtering is a potential XSS vulnerability, allowing arbitrary JavaScript to run in the victim'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 10

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

Question:

List two ways in which an intrusion detection system can support the detection and defence against attacks on a computer system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can confirm whether an attack succeeded or failed by examining host-based IDS log entries.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported	0.25 LOW
2	A passive detection system can log events and raise alerts once an attack has been identified.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::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: 062 - Intrusion Detection System, slide 14; 062 - Intrusion Detection System, slide 29

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

Question:

Refer to your answer in (a). Explain how the distinction between a threat and an attack, together with the role of vulnerabilities, shapes the countermeasures a security team should deploy against malware and other threat classes.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A threat is only a potential violation of security, so countermeasures must anticipate danger before any actual breach occurs.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	partly supported	0.29 LOW
2	An attack is the actual violation of security, so countermeasures must also detect and respond once exploitation happens.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	partly supported	0.33 LOW
3	Because a threat is an entity representing constant danger to an asset, countermeasures must be continuous rather than one-off.	[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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Because an attack deliberately exploits a vulnerability, patching or removing weaknesses is itself a countermeasure.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	partly supported	0.40 LOW
5	Protection of assets must combine prevention, detection and response techniques rather than relying on a single control.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported	0.46 LOW
6	Countermeasures should follow defense-in-depth and a layered security architecture so that one failed layer does not expose the asset.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	partly supported	0.39 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 28; 011 - Introduction to Computer Security, slide 9

PART B - QUESTION 1

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

Scenario:

A software house is drafting a code of ethics for its security team. A junior developer asks why the team cannot simply rely on the ACM code, and a manager wants to know what such a documented code can and cannot achieve for the group.

Question:

Explain what a documented code of ethics provides to a professional group, and discuss the limitations such a code has when guiding the ethical conduct of its members.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code of ethics is a written record of the behaviours that a professional or social group considers acceptable.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.40 LOW
2	The code is established by the group itself rather than imposed from outside.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.12 LOW
3	The code spells out which particular actions are acceptable and which are not.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.14 LOW
4	A limitation is that the code may fail to capture the ethical views held by every individual in the group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.36 LOW
5	Another limitation is that the code often cannot be enforced, since it is a code of conduct and not a legal document.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported (stem gate)	0.55

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 6; 071 - Ethics and Computer Security, slide 9

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

Question:

Referring to the scenario, explain five ethical concerns the security team's code of ethics should address when handling personal information, and why the organization itself, not only individual developers, must take responsibility for protecting that information.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The code should require the team to protect individuals' personal information as a privacy obligation.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	partly supported	0.30 LOW
2	The code should address the accuracy of information, covering authentication and fidelity of the data held.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported	0.30 LOW
3	The code should settle who owns information about individuals and how it may be sold or exchanged.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.64
4	The code should define what information a person has a right to obtain about others and how it may be used.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.64
5	The organization should adopt a recognized professional code of ethics and conduct, such as the ACM code, as the basis for its own responsibility.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.39 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 13; 071 - Ethics and Computer Security, slide 7

PART B - QUESTION 2

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

Scenario:

A system administrator is reviewing how the Linux servers in a campus laboratory protect user accounts. She wants to strengthen the controls applied to password files and login behaviour, and is also concerned about how passwords are stored in encrypted form.

Question:

State FIVE (5) password security controls that can be applied to protect user accounts, and state how a password is stored in encrypted form.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control should be applied to password files.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.67
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
3	The time of the last login should be displayed 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)	0.67
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	The password is stored 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:

Referring to the scenario, the administrator considers deploying Kerberos and single sign-on so that laboratory users authenticate once and are not burdened by repeated password entry. Discuss the motivation for single sign-on and the design criteria that Kerberos must satisfy, and explain how a user's password is used at login.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden of remembering many passwords.	[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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Kerberos must be secure against eavesdropping, so no password is sent in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.67
4	Kerberos must be 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)	0.70
5	At login the hash of the user's password becomes the client's secret key.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.86

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

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

Citations: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 19

End of marking scheme.