KAPASA MAKASA UNIVERSITY LIBRARY

CYBER SECURITY

PAST EXAMINATION PAPERS

FIRST YEAR

2024 AND 2023

SECOND YEAR

2023

THIRD YEAR

2024

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 110 FINAL EXAM

14th OCTOBER 2024

TIME: 09:00 – 12:00 HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 6 Questions, **Attempt any 4 questions including question 1.**

Question 1 is compulsory and carries 40 Marks.

Question 2 – 6 Carries 20 Marks each

Write your answers clearly

Time allowed is **3 hours** only

Only calculators are allowed in the Exam room.

[QUESTION 1]

A. In your opinion, which one is the most important goal from amongst the goals of network security? Convincingly articulate your argument. [3]

B. Using AES algorithm, encode the following hexadecimal message sent using Rinjndael Algorithm. The S-Box, Round Key, initial state array and Predefined matrix are given below. Clearly show the four steps in the first round to get the final sate array in Round one. The S-box, predefined key, initial state array and the round key are given on the last page. [37]

[Total 40 Marks]

[QUESTION 2]

A. Using the RSA encryption algorithm, pick p = 5 and q = 7. Find a set of encryption/decryption keys e and d. **The two keys should be different.** [4]

B. Using the keys that you have found encrypt the word **WORK HARD** assuming that the alphabet is between 1 and 26. [8]

C. Use the decryption key you obtained above to decrypt the cipher text **QOANXFOAWI.** [8]

[QUESTION 3]

A. The centurion who was supposed to inform you of s was killed en route, but you have received the message **VGFRVUREVCNFFBEVSNVY** in a Caesar cipher. Find the value of s and decode the message. Hint: *Use brute force* [5]

B. Your junior course mate asks you to help him decode the message **YANETICGCBETPPNAHSTHOSAARRAERHOYTINB** he has just received from their CYS 110 lecturer. Use columnar transposition cipher to decode and give him the answer using the key **QUARTZ** [5]

C. Using a Caesars cipher with S = 3 and S = 9, Encrypt the message **ACCURACY IS CARDINAL** using a C1C2C2C1C2 sequence [5]

D. The three blocks of hexadecimal numbers **24 45 37, 64 44 A1** and **3B 22 09** need to be hushed in order to get a check sum so that the information they contain maintains its integrity. Calculate the checksum using hexadecimal addition. [5]

[QUESTION 4]

A. You need to encode the message **ATTACK** using a block encoding scheme with the encoding matrix, shown below [5]

$$M = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \quad M' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix}$$

B. Prove that M x M' = $\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$ [5]

C. Using the RSA encryption algorithm, let p = 3 and q =5. Then n = 15 and m = 8. Find the encryption and decryption keys. [5]

D. You receive a message **QYNKERYF** encoded with the block cipher above. Decode to get the original message. [5]

[QUESTION 5]

A. Use columnar transposition to decode the message from your lecture below
TWUSSOHHRETSIECCOESROOABIEUMCYSORELE [5]

B. You are required to encrypt the message "**All the best wishes in your Exams**" using a symmetric key k = 26. Show your work clearly. [5]

C. Convert the following base ten numbers into hexadecimal numbers, 23, 17, 28, 68, and 56. [5]

D. Shimumbi decides to encrypt his already encrypted message with his private key and send to Banamumbi. Explain why he had to do that. [5]

[QUESTION 6]

A. Using RSA, block encoding scheme and stream cipher, encode the word **NEVER DISPAIRE**. For RSA p = 5 and q = 7, for the block encoding use M' in question 4A. The key for the stream cipher keys are S = 4 and S = 6 with sequence C2C1C1C2C2. Note that the output of RSA is fed to the Block Cipher whose output is consequently fed to the stream cipher to get the final cipher text. **For RSA, private and public keys should be different.** [20]

ALL THE BEST WISHES

THE END

S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Predefined Key

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Initial State Array

EA	04	65	85
83	45	5D	96
56	33	98	B0
F0	2D	AD	C5

Round Key

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

SECURE SOFTWARE ENGINEERING
CYS 111

SESSIONAL EXAMINATION

DATE: 31-Oct-24 TIME: 14.00 - 17.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Six (6) questions** in this paper. Attempt only any **five (5).**
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets [ ] at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION ONE

a) What do you understand the term prototyping and give two advantages and disadvantages?

5Marks

b) What is the significance of the closed system concept in software engineering?

3Marks

c) Name Four types of system Testing and why do we test systems

9Marks

d) What is the main reasons for evaluation during system maintenance?

3Marks

QUESTION TWO

a) Explain six core processes required in the development of any new application?

6 Marks

b) i. In life, a system can be ether open or closed. State what is the difference between closed and open systems give one example of each system?

4 Marks

ii. Draw well labeled diagram of Closed and Open system.

4 Marks

iii) explain any three types of information system

6 Marks

QUESTION THREE

a) As a software engineer, why is it necessary to consider the confidentiality of our clients:

6 Marks

b) Draw well labeled diagram and explain each stages of the traditional system development life cycle (waterfall model)

10 Marks

c) Name three main issues that the functional requirements report should outline:

4 Marks

QUESTION FOUR

a) Name three advantages of waterfall model?

6 Marks

b) what are the strengths, weaknesses, and limitations of using development methodologies?

6 Marks

c) What is the significance of the closed system concept in software engineering? **4 Marks**

d) What is the difference between deterministic systems and self-organising systems? **4 Marks**

QUESTION FIVE

a) Explain why organizations initiate information system projects?

3Marks

b) You have just been employed by a company as a Software engineer and they what to embark on developing the new system and you have been asked to be part of the committee that is selecting system projects be embarked on. List and explain the main sources of information systems projects in the organizations?

7Marks

c) Explain the criteria used in organisations when selecting information system projects to invest in

7Marks

d) There are various kinds of committees that select projects. Name any three.

3 Marks

QUESTION SIX

a) What do you understand from the term 'system`s entropy'?

2Marks

b) The process framework encompasses a set of umbrella activities that are applicable across the entire software process. A generic process framework for software engineering encompasses five activities: List and explain these activities?

10Marks

c) You have been on the committee to select projects but you noted that the same project failed feasibility. State any four (4) things that can be done to projects that fail feasibility test?

4Marks

d) State any two (2) reasons why we need to apply standards when approving the feasibility study.

4Marks

END OF EXAM

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 FINAL EXAMS

21ST OCTOBER, 2024

TIME 14:00 – 17:00HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 6 Questions

Attempt a total of 4 questions.

Question 1 is compulsory and carries 40 Marks.

Question 2 – 6 Carries 20 Marks each

Write your answers clearly

Time allowed is **3 hours** only

Only calculators are allowed in the Exam room.

[QUESTION 1]

As network Engineer for NET Consultancy Limited, you have been hired by the Bank of Zambia to carry out a network design and implementation. Apart from the Ndola and Lusaka offices, BOZ has also opened a new office in Livingstone which will have 1008 hosts while the Lusaka and Ndola branches will have 420 and 250 hosts respectively using **172.16.0.0/16**

i. Use VLSM to subnet the internetwork showing clearly the network addresses, the valid hosts and broadcast addresses for each subnet assuming three WAN links connect the three offices. **[20 Marks]**

ii. If the branch managers want to have virtual private networks for their weekly meeting, how many SAs should be created? Justify your answer. **[5 Marks]**

iii. Clearly explain how the Router between Lusaka and Livingstone converts the "original IPv4 datagram" into an IPsec datagram. **[5 Marks]**

iv. Explain the four stages of the 802.11i framework stating how separating the authentication server from the AP allows one authentication server to serve many Aps in a wireless network. Use diagrams where appropriate. **[10 Marks]**

[QUESTION 2]

A. Mention and describe any two cyber-attacks following under each of the following categories **[8]**

I. Social engineering attacks
II. Malware attacks
III. Active Attacks
IV. Passive Attacks

B. A packet segment has amongst other things the SYN field and source IP address Field. At what layer do you find the network element that processes the packet? Explain your answer. **[3]**

C. Explain any two draw backs of symmetric-key system despite being easy and faster compared to asymmetric-key system. **[4]**

D. List the steps that are taken in order to come up with the public and private key in RSA. **[5]**

[Total 20 Marks]

[QUESTION 3]

A. What attacks are avoided by the following methods and how? **[4]**

I. Nonce (OTP)
II. Sequence Number

B. Explain how the following attacks can be avoided. **[5]**

I. Tampering attack
II. Truncation attack

C. Use a table to give any three comparisons between PGP and a S/MIME **[3]**

D. The Client named Alice and Server called Bob want to use Diffie-Helman Key Exchange to exchange a symmetric key that they are going to use to share information over the public communication Channel. If they have selected the prime modular p of 7.

I. Select the generator g that will result in a common shared key of the form g mod p **[2]**

II. Show how you can use the shared key g mod n to come up with final secrete symmetric key that will be used to encrypt the message. Show your calculations clearly. [6]

[Total 20 Marks]

[QUESTION 4]

A. Explain why Bob and Alice might sometimes choose to use a MAC over a Digital signature to carry out authentication. **[3]**

B. Alice intends to send a message **m** to Bob but wants to make sure that the message has **integrity** and is both **authenticated** and **confidential** before sending it. Explain how would achieve the following using appropriate diagrams. **[12]**

I. Message Integrity
II. Authentication
III. Confidentiality
IV. Non-Repudiation

C. Before sending the message **Haris Beats Trump,** you are required to use a check sum algorithm and hash the message to get a message digest. What would be hash message? You might need to use ASCII to help you with your calculations. **[5]**

[QUESTION 5]

A. What is the function of a fire wall in a network security? Hence list and explain the three goals of a fire wall. **[5]**

B. Firewalls can be classified in three primary categories. List and explain each one of them. **[6]**

C. Explain the importance of having an Intrusion Detection System in a Network and how they can be classified. **[3]**

D. Kalebwangu is an online business that students at Kapasa Makasa use to buy commodities they want and can be brought to their do stops. Highlight how SSL (TLS version 3) can be used to prevent Trudy from playing any Man in the middle attack. **[6]**

[QUESTION 6]

A. Clearly give the differences between the following terminologies used in network security **[10]**

I. Message Digest and Message Authentication Code (MAC)
II. Packet analysis and Packet Sniffing
III. Message Authentication and End Point Authentication
IV. A switch and a Router
V. TCP and UDP

B. A virus attacks a single user's computer and within one hour embeds itself in 80 e-mail attachment files sent out to other users. By the end of the hour, 10% of these have been opened and have infected their host machines. If this process continues, how many machines will be infected at the end of 5 hours? Can you find a formula for the number of machines infected after n hours? **[5]**

C. Why do we need network security? **[2]**

D. List the function(S) of each of the following three of the seven layers of the OSI model **[3]**

I. Transport Layer
II. Network Layer
III. Data Link Layer

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

NETWORK DESIGN AND ADMINISTRATION

CYS 100

SESSIONAL EXAMINATION

DATE: 29-Oct-24 TIME: 09.00 - 12.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Seven (7) questions** in this paper. Attempt only **five (5).** **Questions 1 and 2 are compulsory**
3. Indicate on the Answer sheet your choice from the optional questions.
4. Write your Answers on the answer Sheet provided.
5. No Foreign material will be allowed in this examination.
6. The number of marks is shown in brackets [ ] at the end of each question or part question.
7. Clear handwriting and neat work is encouraged.
8. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

[Question 1]

A. Explain the concept of resource sharing in computer networking. How has the growth of the Internet impacted resource sharing? **[5 Marks]**

B. Describe three types of transmission media used in computer networks. **[9 Marks]**

i. Copper wires (shielded and unshielded twisted pair)
ii. Optic fibres
iii. Satellites (Geo-synchronous and Low Earth Orbit)

C. Explain the concept of noise in data communication and its impact on network performance. Describe two techniques that can be used to mitigate the effects of noise in digital communications? **6 Marks]**

[Question 2]

A. Given the IP address 192.168.1.0/24 **[6 Marks]**

i. Write the subnet mask in dotted decimal notation.
ii. Calculate the number of usable host addresses in this network.
iii. Identify the network address and broadcast address.

B. An organization has been assigned the network address 172.16.0.0/16. They need to create 8 subnets of equal size **[9 Marks]**

i. Calculate the subnet mask for each subnet in dotted decimal notation.
ii. Determine the number of usable host addresses per subnet.
iii. List the network address and broadcast address for the first and last subnet.

C. Explain the purpose of subnetting in IP networks. What are the benefits of dividing a large network into smaller subnets? **[5 Marks]**

[Question 3]

A. What is the role of modems in long-distance data communication? Explain the process of modulation and demodulation. **[6 Marks]**

B. Compare and contrast baseband and broadband technologies in data communication. Provide an example application for each. **[8 Marks]**

C. Explain the concept of multiplexing in data communication. Describe two common multiplexing techniques. **[6 Marks]**

[Question 4]

A. What are packets in data communication? Explain how packets enable time-division multiplexing. **[5 Marks]**

B. Describe the following error detection techniques used in data communication **[9 Marks]**

i. Parity checking
ii. Checksums
iii. Cyclic redundancy checks (CRC)

C. What is the purpose of byte stuffing in data framing? Provide an example to illustrate how byte stuffing works. **[6 Marks]**

[Question 5]

A. Compare and contrast direct point-to-point and shared communication channels in LAN technologies. **[4 Marks]**

B. Describe any three main LAN topologies, and discuss the advantages and disadvantages of each of those topologies **[12 Marks]**

C. Explain the concept of Carrier Sense Multiple Access (CSMA) and its role in managing network traffic on shared media. **[4 Marks]**

[Question 6]

A. What is the purpose of hardware addressing in LANs? Explain the format of physical addresses and the concept of multicast addressing. **[6 Marks]**

B. Describe the following Ethernet wiring schemes. Discuss the advantages and disadvantages of each scheme. **[9 Marks]**

i. Thick Ethernet
ii. ii. Thin Ethernet
iii. iii. Twisted Pair Ethernet

C. Explain the role of Network Interface Cards (NICs) in LAN communication. What factors should be considered when selecting a NIC for a network device? **[5 Marks]**

[Question 7]

A. What are the distance limitations of LANs? How can fibre optic extensions and repeaters help overcome these limitations? **[5 Marks]**

B. Explain the purpose and function of the following network devices **[9 Marks]**

i. Bridges
ii. Switches
iii. Routers

C. Compare and contrast the following network types. Provide an example use case for each type of network. **[6 Marks]**

i. Local Area Network (LAN)
ii. Wide Area Network (WAN)
iii. Metropolitan Area Network (MAN)

The End
All the best!

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 FINAL EXAMS

21ST OCTOBER, 2024

TIME 14:00 – 17:00HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 6 Questions

Attempt a total of 4 questions.

Question 1 is compulsory and carries 40 Marks.

Question 2 – 6 Carries 20 Marks each

Write your answers clearly

Time allowed is **3 hours** only

Only calculators are allowed in the Exam room.

[QUESTION 1]

As network Engineer for NET Consultancy Limited, you have been hired by the Bank of Zambia to carry out a network design and implementation. Apart from the Ndola and Lusaka offices, BOZ has also opened a new office in Livingstone which will have 1008 hosts while the Lusaka and Ndola branches will have 420 and 250 hosts respectively using **172.16.0.0/16**

i. Use VLSM to subnet the internetwork showing clearly the network addresses, the valid hosts and broadcast addresses for each subnet assuming three WAN links connect the three offices. **[20 Marks]**

ii. If the branch managers want to have virtual private networks for their weekly meeting, how many SAs should be created? Justify your answer. **[5 Marks]**

iii. Clearly explain how the Router between Lusaka and Livingstone converts the "original IPv4 datagram" into an IPsec datagram. **[5 Marks]**

iv. Explain the four stages of the 802.11i framework stating how separating the authentication server from the AP allows one authentication server to serve many Aps in a wireless network. Use diagrams where appropriate. **[10 Marks]**

[QUESTION 2]

A. Mention and describe any two cyber-attacks following under each of the following categories **[8]**

I. Social engineering attacks
II. Malware attacks
III. Active Attacks
IV. Passive Attacks

B. A packet segment has amongst other things the SYN field and source IP address Field. At what layer do you find the network element that processes the packet? Explain your answer. **[3]**

C. Explain any two draw backs of symmetric-key system despite being easy and faster compared to asymmetric-key system. **[4]**

D. List the steps that are taken in order to come up with the public and private key in RSA. **[5]**

[Total 20 Marks]

[QUESTION 3]

A. What attacks are avoided by the following methods and how? **[4]**
I. Nonce (OTP)
II. Sequence Number

B. Explain how the following attacks can be avoided. **[5]**
I. Tampering attack
II. Truncation attack

C. Use a table to give any three comparisons between PGP and a S/MIME **[3]**

D. The Client named Alice and Server called Bob want to use Diffie-Helman Key Exchange to exchange a symmetric key that they are going to use to share information over the public communication Channel. If they have selected the prime modular p of 7.
I. Select the generator g that will result in a common shared key of the form g mod p **[2]**

II. Show how you can use the shared key g mod n to come up with final secrete symmetric key that will be used to encrypt the message. Show your calculations clearly. [6]

[Total 20 Marks]

[QUESTION 4]

A. Explain why Bob and Alice might sometimes choose to use a MAC over a Digital signature to carry out authentication. [3]

B. Alice intends to send a message **m** to Bob but wants to make sure that the message has **integrity** and is both **authenticated** and **confidential** before sending it. Explain how would achieve the following using appropriate diagrams. [12]

I. Message Integrity
II. Authentication
III. Confidentiality
IV. Non-Repudiation

C. Before sending the message **Haris Beats Trump,** you are required to use a check sum algorithm and hash the message to get a message digest. What would be hash message? You might need to use ASCII to help you with your calculations. [5]

[QUESTION 5]

A. What is the function of a fire wall in a network security? Hence list and explain the three goals of a fire wall. [5]

B. Firewalls can be classified in three primary categories. List and explain each one of them. [6]

C. Explain the importance of having an Intrusion Detection System in a Network and how they can be classified. [3]

D. Kalebwangu is an online business that students at Kapasa Makasa use to buy commodities they want and can be brought to their do stops. Highlight how SSL (TLS version 3) can be used to prevent Trudy from playing any Man in the middle attack. [6]

[QUESTION 6]

A. Clearly give the differences between the following terminologies used in network security [10]

I. Message Digest and Message Authentication Code (MAC)
II. Packet analysis and Packet Sniffing
III. Message Authentication and End Point Authentication
IV. A switch and a Router
V. TCP and UDP

B. A virus attacks a single user's computer and within one hour embeds itself in 80 e-mail attachment files sent out to other users. By the end of the hour, 10% of these have been opened and have infected their host machines. If this process continues, how many machines will be infected at the end of 5 hours? Can you find a formula for the number of machines infected after n hours? [5]

C. Why do we need network security? [2]

D. List the function(S) of each of the following three of the seven layers of the OSI model [3]

I. Transport Layer
II. Network Layer
III. Data Link Layer

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BARCHELOR OF SCIENCE IN CYBER SECURITY

CYS 121 - INFORMATION SYSTEMS SECURITY

SESSIONAL EXAMINATIONS

Date: 5th November,2024. **Time: 3 hours**

Total Marks: 100

Instructions to Candidates:

There are three (3) sections in this paper.

- SECTION A: Answer all questions in this section. 10 Marks
- SECTION B: Answer all questions in this section. 30 Marks
- SECTION C: Answer question 1 and choose any two 60 Marks

Write your student Identification Number on the Answer Booklet provided.

Calculators are allowed.

SECTION A [10 MARKS]

1. A program designed to destroy data on your computer which can travel to "infect" other computers is called a _?

A. Disease
B. Torpedo
C. Hurricane
D. Virus

2. Software such as viruses, worms and trojan horses that has malicious intent is known as .....

A. Spyware
B. Adware
C. Spam
D. Malware

3. An act to injure, corrupt or threaten a system or network is characterized as which of the listed below?

A. Digital crime
B. Threats
C. System hijacking
D. Cyber-attack.

4. Which of the following statements best describes how the principle would be broken if a computer was no longer accessible?

A. Confidentiality
B. Access control
C. Availability
D. Denial

5. Which of the following is a method of hiding information inside a picture?

A. Image rendering
B. Steganography
C. Rootkits
D. Bitmapping

6. They are malicious hackers whose primary goal is to commit cybercrimes to make money. Who are they in this context?

A. White Hat hackers
B. Black Hat hackers
C. Hacktivists
D. Gray Hat hackers

7. What is changed when cypher algorithms are used?

A. Scalar text
B. Plain text
C. Complex text
D. Cipher text

8. A person who uses his or her expertise to gain access to other people's computers to get information illegally or do damage is called a?
A. Hacker
B. Analyst
C. Spammer
D. Programmer.

9. A _____ can be a hardware device or software program that filters all the packets of data that comes through a network, the internet etc.
A. Firewall
B. Antivirus
C. Malware
D. Cookies

10. The process of encoding data to protect it from unauthorized access is known as ____?
A. Encryption
B. Firewall
C. Intrusion detection
D. Multi-factor authentication.

SECTION B [30 MARKS]

Answer all questions in this section.

1. Write short notes on the following types of attacks;
   i. Denial-of-service attacks (DoS) [4 marks]
   ii. Spoofing [4 marks]
   iii. Man In middle attack [4 marks]
   iv. Sniffing [4 marks]
   v. Masquerading [4 marks]

2. With the help of diagrams explain what Denial of service Attack (DoS) and Distributed Denial of Service Attack (DDoS) is. [10 marks]

SECTION C [60 MARKS]

Answer three (3) questions from this section. Question 1 is a compulsory question

1. Explain the difference between viruses, worms, Trojan horses, and ransomware. How do they operate and differ in their spread? [20 marks]

2. What are **zero-day** exploits and how do they pose a unique challenge for cybersecurity professionals? Discuss mitigation strategies. [20 marks]

3. Discuss the CIA triad in relation to cyber security. Use relevant examples in your explanation. [20 marks]

4. Encrypt "**freedom has come** "using the substitution technique method of Caesar Cipher, use the key = 3. Show all the steps of your working. [20 marks]

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

COMMUNICATION SKILLS
CYS 122

SESSIONAL EXAMINATION

DATE: 25-Oct-24 TIME: 09.00 - 12.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Seven (7) questions** in this paper. Attempt any **five (5).** Indicate on the Answer sheet your choice from the optional questions.
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets [ ] at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. Incorrect spellings and wrong grammar will result in loss of marks.
8. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION ONE (1): INTRODUCTION TO COMMUNICATION SKILLS AND PROTOCOL

(a) With the help of a communication model (diagram), outline the Communication Process. (10 marks)

(b) Discuss some consequences of poor Communication and Protocol Breaches in Cybersecurity or any other field. (10 marks)

QUESTION TWO (2): VERBAL AND NON VERBAL COMMUNICATION AND COMMUNICATION IN LEADERSHIP

(a) Suggest oral (verbal) ways of preventing and resolving conflicts in the work- place. (10 marks).
(b) Explain some cultural differences that may be encountered during non-verbal Communication (10 marks).

QUESTION THREE (3): WRITTEN COMMUNICATION

As Chairperson of the Cybersecurity Society at Kapasa Makasa University, you attended a workshop which was reviewing the Zambia Cybersecurity and Cyber Crimes Act Number 2 of 2021.

You took down the following points:

- The Zambia Cybersecurity and Crimes Act seeks to:

- Provide for cybersecurity in Zambia
- Ensure protection of persons against Cybercrimes, including online child protection
- Facilitate the identification, declaration and protection of critical information infrastructure
- Promote the responsible use of social media Platforms
- Foster the creation of a secure, reliable and trustworthy cyber environment that increases confidence.

Using the points above and any of your own, write a report to the Head of Department for I. C.T. about the purpose of the Zambia Cybersecurity and Cyber Crimes Act of 2021.

Remember to include a recommendation. (20 marks)

QUESTION FOUR (4): SPECIALISED (BUSINESS) COMMUNICATION SKILLS

(a) Write a letter addressed to the Chief Executive Officer of ABSA Bank Headquarters in Lusaka on P.O. Box 500163, applying for the advertised vacant post of Cybersecurity Specialist.

Briefly state your age, education background, qualifications, experience, hobbies and referees. (10 marks)

(c) Enclose your one paged Curriculum Vitae (CV). (10 marks)

QUESTION 5: PROTOCOL, ETIQUETTE AND DIGITAL COMMUNICATION NETIQUETTE

With appropriate examples, distinguish between etiquette and netiquette. (20 marks)

QUESTION SIX (6): SPECIALISED VERBAL COMMUNICATION

(a) State any five (5) things you would do to adequately prepare for an oral job interview, and write five (5) points about how you would conduct yourself during the oral interview for a Cybersecurity Specialist at ZAMTEL. (10 marks)
(b) With appropriate examples, propose workable strategies you would use to effectively handle crisis Communication at your institution or place of work. (10 marks)

QUESTION SEVEN (7: WRITTEN COMMUNICATION

With at least one example on each agenda item, formulate the layout of meeting minutes from the title to the adjournment of the meeting. (20 marks)

THE END!

KAPASA MAKASA UNIVERSITY
PAST EXAMINATION PAPERS
2023

DEPARTMENT OF ICT
FIRST YEAR CYS

COURSE CODE:

CYS 110

CYS 120

CYS 111

CYS 121

CYS 100

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES AND EDUCATION

2023 SESSIONAL EXAMINATION

CS 110 – INTRODUCTION TO COMPUTING

INSTRUCTIONS

(1) Time allowed is **Three (3) hours**.
(2) There are six questions in this paper. **Answer any five (5) questions.**
(3) Each question carries **20 Marks**.

Ecclesiastes 9 vs 10-11

DO NOT TURN THIS PAGE UNTIL YOU ARE

QUESTION ONE

Explain the current trends in the field of computing as learnt in class. [12 Marks]

A *computer* is an electronic machine that accepts data from the user, processes the data by performing calculations and operations on it, and generates the desired output results. Imagine you have been given an LCD monitor, a mouse, keyboard and an empty computer case by a friend. You know components that are supposed to be put inside the case so that your computer becomes functional. Ignore all the cables, PCI cards and the CD ROM;

a) List 6 components that you can buy from a shop to complete the unit, without which the computer cannot work. [2 Marks]
b) From the components you have listed in (a), Choose any four (4) and provide acceptable specifications that you can look for. [2 Marks]
c) What do the acronyms LCD stand for in LCD Monitor? [2 Marks]
d) True/False – You can mix the components you have listed in (a) regardless of the vendor and the computer can work. [2 Marks]

QUESTION TWO

a) Computer memory is organized in form of a hierarchy based on three competing properties, namely Cost, Size and speed. Draw the memory hierarchy that is used in computers. **[2 Marks]**

b) From the following list, cross out the invalid ones and mark the valid ones. **[5 Marks]**
   a. 1001101_{10}
   b. 12777_{8}
   c. $ABCDFE_{16}$
   d. $FEED_{16}$
   e. 01100012111000100_{2}
c) Convert the value 2049_{10} directly to base 8, then from base 8 directly to base 2, then from base 2 directly to base 16, and then from base 16 directly back to base 10. **[8 Marks]**
d) Convert $FD27_{16}$ to base 2 represented as a 32 bit value. **[3 Marks]**

e) Identify the following network topologies: **[2 marks]**
   a. Each device has a receiver and transmitter to receive the data signals and to send them to the next computer, respectively.
   b. A single coaxial cable is generally used, to which the computers or devices are connected. **[2 Marks]**

QUESTION THREE

a) A sales person may manage many other salespeople. A salesperson is managed by only one sales people. A salesperson can be an agent for many customers. A customer is managed by one sales people. A customer can place many orders. An order can be placed by one customer. An order lists many inventory items. An inventory item maybe listed on many orders. An inventory item is assembled from many parts. A part may be assembled into many inventory items. Many employees assemble an inventory item from many parts. A supplier supplies many parts. Draw the Entity- Relationship Diagram (ERD) for the above scenario. **[10 Marks]**

b) Draw an FR diagram for the following application from the ABC Company: **[10 Marks]**

1. Employees work for many projects and each project has many employees
2. Each employee has an unique Emp_No
3. Each employee has a name and name consists of first name, middle name andlast name
4. Each project has an unique number and name

QUESTION FOUR

Fill in the blanks. [1 Marks Each]

a) _____ is an inference or conclusion drawn from the information.

b) A _____is a security mechanism to protect a local network from the threats it may face while interacting with other networks (Internet).

c) A _____ name is a unique name that identifies a particular website and represents the name of the server where the web pages reside.

d) Since _____ systems are integrated systems: they help to streamline different processes and workflows, allow data to be easily shared across various departments in an organization, improve the efficiency and productivity levels, and improves customer service.

e) The _____is a collection of linked documents or pages stored on millions of computers and distributed across the world.

f) The most critical aspect of the modem is its speed of operation. The speed of modem is measured in_____

g) ISDN is an acronym for _____

h) The software that is intentionally included into a system with the intention to harm the system is called malicious software or _____ in short.

i) As a type of Information Systems, ERP stands for _____

j) A_____ is self-replicating software that uses network and security holes to replicate itself.
k) XML is an acronym for _____.

l) Expert system is an applied area of Artificial Intelligence. An expert system is a knowledge- based system having two main components – knowledge base and _____.
m) _____ are destructive programs that masquerade as useful programs.
n) A program that traverses the Web from link to link, identifying and reading pages is called _____.
o) _____virus infects both boot sectors and executable files, and uses both mechanisms to spread
p) As a characteristic of computers, _____ implies that when used for a longer period of time, the computer does not get tired or fatigued.
q) In relation to computer cables, IDE stands for _____
r) _____ is an optical disc storage medium designed to supersede the DVD format.
s) Conditions necessary for a deadlock includes Circular Wait, Hold and Wait, No preemption and _____
t) The capacity of a conventional DVD is _____.

QUESTION FIVE

Carefully examine the 20 statements given below. Some of them are true, others are false. Indicate which ones are true and which ones are false. Marks for each point will be awarded as +1 for correct, -1 for incorrect, and 0 for un-attempted.

a) A *digital computer* uses distinct values to represent the data internally. All information is represented using the digits 0s and 1s. The computers we learnt in this course are digital computers.
b) The fourth generation computers are based on *Artificial Intelligence (AI)*. They try to simulate the human way of thinking and reasoning.
c) Fetching, decoding and executing are the three stages that make up the instruction cycle.
d) When booting, the computer performs a Power On Self Test (POST) that checks that the software is functioning properly and the Operating System is present.
e) Flash Disks uses a kind of semiconductor-based non-volatile, rewritable computer memory that can be electrically erased and reprogrammed. It is a specific type of EEPROM.
f) MICR stands for Magnetic Ink Character Recognition.

g) Ink-jet printer is an example of impact printers.
h) Application software provides basic functionality to the computer. Application software is required for the working of computer itself. The user of computer does not need to be aware about the functioning of Application software, while using the computer.
i) A device driver acts as a translator between the hardware and the software that uses the devices. In other words, it hardware that intermediates between the device and the software, in order to use the device.
j) Public Domain Software is free software. However, public domain software does not have a copyright owner or license restrictions. The source code is publicly available for anyone to use. Public domain software can be modified by the user.
k) A *race condition* is a situation when a process waits endlessly for a resource and the requested resource is being used by another process that is waiting for some other resource.
l) Microwave transmission refers to the technique of transmitting information over a microwave link. Microwaves have a higher frequency than radio waves. They are line-of-sight.
m) The World Wide Web (abbreviated as the Web or WWW) is a collection of linked documents or pages, stored on millions of computers and distributed across the world. Although the WWW is often referred to as the Internet, they are actually two different concepts. The Internet is one of the most popular services available on the World Wide Web.
n) A web page is written in a language called HTML (Hypertext Makeup Language).
o) The hyperlink is a system that provides a simple and consistent way of organizing large data (that includes text, images, pictures and videos) available on the Internet
p) Stealth virus, unlike other viruses, consists of static virus program that gets copied from file to file as it propagates. Such virus is difficult to detect because each copy it generates, appears different from the other one. It uses encryption algorithm to multiply new copies of the program
q) DSS provides a generalized computing and communication environment to senior managers to support strategic decisions. It provides summarized information in a convenient form to the top level managers. Unlike EIS, they are not designed to use analytical models for specific problem solving.
r) A modem (i.e. modulator-demodulator) is a hardware, which converts analog signal into digital data (i.e. modulation) that can be sent over a digital telephone line and convert the digital data back into analog signal (i.e. demodulation)
s) The standard protocol used for sending e- mail is called SMTP (Simple Mail Transfer Protocol). It works in conjunction with POP (Post Office Protocol) and IEAP (Internet Email Access Protocol) servers.
t) A worm can modify a program just like a virus; it also replicates so much that it consumes the resources of the computer and makes it slow.

QUESTION SIX

Write short notes on the following computing concepts.

a) Virtual Memory
b) Public Key Cryptography
c) Enterprise Resource Planning (ERP)
d) Computer Output on Microfiche. [5 Marks Each]

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES AND EDUCATION

2023 SESSIONAL EXAMINATION

CYS100 – NETWORK DESIGN AND ADMINISTRATION

INSTRUCTIONS

(1) Time allowed is **Three (3) hours**.

(2) There are six questions in this paper. **Answer any five (5) questions.**

(3) Each question carries **20 Marks**.

Ecclesiastes 9 vs 10-11

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO

Question One

i. Discuss the latest trends in the field of cyber security with a particular focus on network design and administration.
[15 Marks]

ii. With regards to network design and administration, explain the difference between logical and physical addressing and give an example in each case.
[5 Marks]

Question Two

i. Briefly explain any two key design issues that a network designer should take into consideration when designing an organization network.
[5 Marks]

ii. Network design and management is an interesting and time consuming job but often considered as the most difficult job in IT. Discuss why?
[5 Marks]

iii. KMU network administrator tabulated bandwidth and throughput and observed the value of bandwidth was constant while throughput was varying. Differentiate between bandwidth from throughput and briefly explain the observation.
[5 Marks]

iv. Describe the process of terminating a straight through cable. **[5 Marks]**

Question Three

a) Describe the role of each of the following tools during either design or implementation of a network project:
[8 Marks]

i. TDR
ii. Crimping tool
iii. Voltmeter
iv. LAN tester

b) Explain why a switch is used to replace a hub in modern networks. **[5 Marks]**

c) Identify and explain two methods that can be used to collect data for a network design project.

[4 Marks]

d) Describe any three network security strategies. **[3 Marks]**

Question Four

a) Identify the three classes used for public IP address and give an example in each case.

[6 Marks]

b) State the layer and explain a design or implementation issue related to any four of the OSI reference model.

[8 Marks]

c) Explain the following terms in reference to Network Interface Card. **[6 Marks]**

i. Physical address is hard coded

ii. ii. Ethernet NIC

iii. iii. Wireless NIC

Question Five

Explain why an organization would chose to implement a client server network architecture to replace a peer to peer architecture. **[7 Marks]**

Network design involve evaluating, understanding and scoping the network to be implemented. Explain the four activities that would be addressed during the network design. **[7 Marks]**

In a table form, differentiate between network management and network troubleshooting. **[6 Marks]**

Question Six

Briefly outline the responsibilities of the network administrator. **[6 Marks]**

Mention at least ten (10) activities that computer network administrator would perform during network management. **[10 Marks]**

KAPASA MAKASA UNIVERSITY

DEPARTMENT OF ICT

CYS 121
Information Systems Security

2023 Sessional Examination

(3 hours 00 minutes)
(100 marks)

INSTRUCTIONS:

- This paper has no sections, and answer all the questions using the answer booklet provided.
- Questions 1 to 14 are mandatory.
- Choose any five questions, from question 15 to question 22
- Be brief in your responses to the questions, and the use of examples is encouraged to help you highlight your point.

The use of calculators or any other computerized device (eg a phone) is not allowed.

1. What is computer and information system security all about? (5)
2. List any five characteristics that information possesses. (5)
3. A security engineer has recently installed a biometric system and needs to tune it. Currently, the biometric system is rejecting too many valid, registered users. What adjustment does the security engineer need to make, justify your response. (5)
4. The four means of authenticating user identity are based on something the individual knows, something the individual possesses, something the individual is, and something the individual does. Give at least a valid example for each of those four. (5)
5. What is access control, and what are the three main concerns of access control? (5)
6. You have been requested to prepare a workshop at Kapasa Makasa University and discuss the Access Control examples. To help you get started, your supervisor has provided the following table, but could not finish before he was called for a meeting by the Vice Chancellor. As his assistant, complete the table below. Directives, and Compensating, everything has been done for you. Pick any two either Deterrent, Preventive, Detective, Corrective or Recovery, and provide two examples for administrative controls and technical controls. (5)

Controls	Administrative	Technical	Physical
Directive	Policy	Warning Banner	'Do Not Enter'
Deterrent			'Beware of Dog'
Preventive			Fences, Bollards
Detective			Sensors, CCTV
Corrective			Fire Extinguisher
Recovery			Reconstruct, Rebuild
Compensating	Supervision, Job Rotation	Keystroke Logging	Layered Defenses

7. The corporate controller of metoyou.com, a commodities trader, purportedly received emails from the CEO of the company (Jeph Kapi) and a Lusaka-based auditing firm that works with the company, requesting three wire transfers to a Chinese bank totalling an estimated one (1) million kwacha (K1,000,000). The emails asked for the controller's discretion as the money was for the acquisition of a Chinese company. The controller complied with the requests, assuming that the CEO directed them, even though the email used was not an official company email. (5)
   a) What type of cybercrime is this?
   b) Justify your response.
8. Give two (2) examples of offences against computer data and systems concerning (5)
   a) Confidentiality
   b) Availability
9. Spam is considered a form of computer-related fraud and a content-related crime. (5)
   a) Define what spam is.
   b) Explain why it is considered both computer-related fraud and a content-related crime
10. Cornish and Clarke (2003) proposed five strategies and 25 techniques (with five techniques under each strategy) to prevent and reduce crime. Below, is a table of cybersecurity techniques that would be to prevent and/or reduce that cybercrime.

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules

Control access to facilities	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce emotional arousal	Alert conscience
Deflect offenders	Utilize place managers	Disrupt markets	Neutralize peer pressure	Assist compliance
Control tools/weapons	Strengthen formal surveillance	Deny benefits	Discourage imitation	Control drugs and alcohol

Are there any techniques that do not apply to cybersecurity? Briefly justify your response. (5)

11. In under a sentence or two, briefly describe the following terms: (10)
    a) an asset
    b) a vulnerability
    c) a risk
    d) Access Authentication
    e) Access controls
12. Using a brief sentence, distinguish (5)
    a) a worm and a virus.
    b) Phishing and whaling
13. Cybersecurity Audit Checklist provides a comprehensive list of items that should be checked out during a security audit. List any of such items that need to be on the checklist. (5)
14. Database watermarking involves aspects of data hashing and digital watermarking, of data stored in a file. Elaborate on the purpose of watermarking. (5)

Choose any five (5) from the questions below:

15. Explain any two of three things that must be considered for the planning and implementation of access control mechanisms, in cyber security. (5)
16. Information System is an entire set of software, hardware, data, people, procedures and networks. Describe any five of those components of an IS. (5)
17. Organization assets and data can be classified into any of the following categories: Unclassified, Sensitive but Unclassified, Confidential, Secret and Top-secret. Describe Confidential, Secret and Top-secret, mentioning whether it requires a court order, government contracts, or senior-level approval to make the assets public. (5)
18. Explain in brief the Role-based Access Control and Temporal Access Control. (5)
19. Denial-of-service or DOS attacks are much more significant in networks than in other contexts, they are accidental and/or caused by malicious threats. Mention any five of the accidental and/or malicious threats that cause DOS attacks. (5)
20. Why and how is the Single Sign-on Kerberos, important as a computer network authentication protocol? (5)
21. Explain in brief, the following malware:
    a) Ransomware
    b) Adware
22. Distinguish between heuristic analysis and sandbox method as security measures against malware. (5)

KAPASA MAKASA UNIVERSITY
COMPUTER SCIENCE DEPARTMENT

SECURE SOFTWARE ENGINEERING

CYS 111

FINAL EXAMINATION

Instructions

i. Time allowed: **3 hours**, Total Marks allocated to each question: **20 Marks**
ii. There **SIX Questions** in this Paper Answer **ANY FIVE** questions.
iii. The marks allocated on each question give a clue as to the depth of you answer.
iv. **Please, where appropriate, use diagrams and/or examples**

QUESTION ONE

a) Explain six core processes required in the development of any new application ?

6 Marks

b) i. In life, a system can be ether open or closed. State what is the difference between closed and open systems give one example of each system?

4 Marks

ii. Draw well labeled diagram of Closed and Open system.

4 Marks

iii) list explain three types of information system

6 Marks

QUESTION TWO

a) What do you understand the term prototyping and give two advantages and disadvantages?

5Marks

b) What is the significance of the closed system concept in software engineering?

3Marks

c) Name Four types of system Testing and why do we test systems

9Marks

d) What is the main reasons for evaluation during system maintenance?

3Marks

QUESTION THREE

a) As a software engineer, why is it necessary to consider the confidentiality of our clients:

6 Marks

b) Draw well labeled diagram and explain each stages of the traditional system development life cycle (waterfall model)

10 Marks

c) Nam three main issues that the functional requirements report should outline:

4 Marks

QUESTION FOUR

a) Name three advantages of waterfall model?

6 Marks

b) what are strengths, weaknesses, and limitations of using development methodologies?

6 Marks

c) What is the significance of the closed system concept in software engineering?

4 Marks

d) What is the difference between deterministic systems and self-organising systems?

4 Marks

QUESTION FIVE

a) Explain why organizations initiate information system projects?

3Marks

b) You have just been employed by a company as a Software engineer and they what to embark on developing the new system and you have been asked to be part of the committee that is selecting system projects be embarked on. List and explain the main sources of information systems projects in the organizations?

7Marks

c) Explain the criteria used in organisations when selecting information system projects to invest in

7Marks

d) There are various kinds of committees that select projects. Name any three.

3 Marks

QUESTION SIX

a) What do you understand the term system's entropy?

2Marks

b) The process framework encompasses a set of umbrella activities that are applicable across the entire software process. A generic process framework for software engineering encompasses five activities: List and explain these activities?

10Marks

c) You have been on the committee to select projects but you noted that same project failed feasibility. State any four (4) things that can be done to projects that fail feasibility test?

4Marks

d) State any two (2) reasons why we need to apply standards when approving the feasibility study.

4Marks

END OF EXAM

KAPASA MAKASA UNIVERSITY
COMPUTER SCIENCE DEPARTMENT

SECURE SOFTWARE ENGINEERING

CYS 111

FINAL EXAMINATION

Instructions

i. Time allowed: **3 hours**, Total Marks allocated to each question: **20 Marks**
ii. There **SIX Questions** in this Paper Answer **ANY FIVE** questions.
iii. The marks allocated on each question give a clue as to the depth of you answer.
iv. **Please, where appropriate, use diagrams and/or examples**

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 DEFERED EXAMS

NOVEMBER 2023

Do not turn this page until you are told to do so

This Question paper contains 7 Questions

Attempt five questions.

Questions 1 and 2 are compulsory

The folder should be named using your student ID

Time allowed is **3 hours** only.

Calculators are allowed in the exam

[QUESTION 1]

A. Zambia National Commercial Bank has a network between Lusaka and Ndola offices as described below. The Ndola office has an accounts server for the accounts department. It then has the HR and Operations department. Each of these departments has 10, 11 and 5 hosts respectively. The Lusaka office has the Admin, Finance and Security departments with 6, 30 and 15 hosts respectively. If the IP Address is **192.168.80.0/24**, use VLSM to subnet the network and show the following
[12 Marks]
   I. The subnetwork Addresses
   II. Show the network design on the paper
   III. The valid host addresses for each subnet
   IV. The broadcast addresses

B. Using OSPF as the routing protocol, write the configurations that you use to ensure internetworking takes place. **[4 Marks]**

C. Use an appropriate access list to block all the departments from accessing the accounts server apart from the Admin and Finance department. **[4 Marks]**

[QUESTION 2]

Chinsali Judiciary has two offices one in New Town and the other one in old Boma. The IT department has just designed their internetwork as shown below. The IT department itself has 16 hosts, 4 at old Boma office and 12 at New Town. Planning department has 10 hosts all located at New Town office, finance department has 5 all located in New Town and finally the Engineering department has 14 hosts with 7 hosts at old Boma and the other 7 at New Town Office. The two offices are connected via a WAN link. As a new Network Administrator you have received the IP Address as **192.168.30.0 255.255.255.0** from MTN your ISP.

A. Subnet the internetwork using VLSM and draw the design of the network. **[5 Marks]**

B. Write the configs that will create a VLAN for each department **[8 Marks]**

C. If you using RIP Version 2 Routing protocol, show the configs that will enable internetworking to take place **[4 Marks]**

D. Using an appropriate access list, configure a fire wall that will block all IP traffic from engineering and planning from going to the finance department. **[3 Marks]**

[QUESTION 3]

A. What is Kerberos? Consequently explain the three different sets of entities that use Kerberos? **[4 Marks]**

B. Explain how you would use Kerberos to authenticate a user wanting to access a printing service on a network. **[6 Marks]**

C. Kapasa Makasa University Students' Union (KAMUSU) has launched an e-commerce agri-business where they are advertising, selling and delivering different products like Maize, Potato, Sunflower and Soya bean seeds to any farmer in the country. Mr. Sampa has just retired from the civil service and has settled in Chipindo resettlement scheme of Bwengwa district, southern province. How can you employ SSL to ensure that KAMUSU

and Mr. Sampa conduct their online business securely? Clearly explain steps that can be taken to ensure Confidentiality, Integrity and Authentication is achieved as well as avoiding connection replays and packet replay attacks. **[8 Marks]**

D.

In the above scenario how can you avoid a truncation attack from taking place? **[2 Marks]**

[QUESTION 4]

A. State the reason why the OSI model was created and hence draw and explain the functions of each layer of the Open System for Interconnections. **[5 Marks]**

B. With the help of the diagram, briefly explain the three broad categories of the **OSI security Architecture.** **[4 Marks]**

C. With the help of a suitable diagram, draw and briefly explain the **Model of Network Security**

[6 Marks]

D. Give definitions for the following terms **[5 Marks]**

I. Message digest
II. Session Key
III. Network Security
IV. Broadband technology
V. DMZ

[QUESTION 5]

A. Alice intends to send a message **m** to Bob but wants to make sure that the **message** has **integrity** and is both **authenticated** and **confidential** before sending it. Explain how she can use symmetric key, public key infrastructure and hush functions like SHA-1 to achieve the above stated goals. Use appropriate diagrams to explain your answer. **[10 Marks]**

B. What is a Message Authentication Code (**MAC**) and how is it created? **[2.5 Marks]**

C. What does the **PGP** abbreviation in the PGP protocol stand for and what is used for? **[2.5 Marks]**

D. Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures. Name two reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. **[5 Marks]**

[QUESTION 6]

A. What is the difference between **passive** and **active** cyber security attacks? Give two examples of each. **[5 Marks]**

B. Differentiate between an attack and a vulnerability **[5 Marks]**

C. Anomaly based and signature based IDSs used to detect a wide range of cyber-attacks. Explain how each one them works describing their differences. **[5 Marks]**

D. List and explain the three types of firewalls that can be used in the network to improve network security. **[5 Marks]**

[QUESTION 7]

A. What do the initials SAD and SPD stand for in an IPsec Virtual Private Network? Hence state the difference between the two. **[4 Marks]**

B. How is an IPv4 datagram converted to an IPsec datagram by the IPsec entity like a router before transmission over the public network? Explain with the use of a diagram. **[8 Marks]**

C. Bank of Zambia has two branches, one in Lusaka and the Ndola office. The Lusaka (HQs) office has 23 hosts and one router and the Ndola (branch) office has one router and 12 hosts. If the institution is using VPN to communicate over the unsecured public network. How many SAs will be in the SAD .Explain your answer? **[3 Marks]**

D. Using appropriate diagrams, explain how you can secure a wireless network using IEEE 802.11i framework. **[5 Marks]**

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 100 DEFRED EXAM

CRYPTOGRAPHY

NOVEMBER 2023

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 7 Questions

Attempt 5 Questions, Questions 1 and 2 are compulsory

All questions carry equal marks

Start each question on a new page.

Time allowed is **3 hours** only

Calculators are allowed in the exam

[QUESTION 1]

A. Using the RSA encryption algorithm, pick p = 11 and q = 7. Find a set of encryption/decryption keys including e and d. **[10 Marks]**

B. Using the private and public keys calculated above, encrypt the word **DEFERED** and provide its cipher text. **[5 Marks]**

C. The three blocks of hexadecimal numbers **29 45 37, 64 46 A1** and **3B 21 09** need to be hushed in order to get a check sum so that the information they contain maintains its integrity. Calculate the checksum using hexadecimal addition. **[5 Marks]**

[QUESTION 2]

A. Using a Caesar cipher with S = 5 decode the received message **YMNX YJXY NX NSYJWJXYNSL.** **[5 Marks]**

B. Using a Caesars cipher with S = 3 and S = 10, Encrypt the message WELCOME TO CRYPTOGRAPHY using a C1C2C2C1C2 sequence **[5 Marks]**

C. The centurion who was supposed to inform you of s was killed en route, but you have received the message **MXX SMGX UE PUHUPQP** in a Caesar cipher. Find the value of s and decode the message. Hint: *Use Brute Force* **[10 Marks]**

[QUESTION 3]

A. You receive a message that was encoded using a block encoding scheme with the encoding matrix, Decode the cipher text MXOSHI

$$M = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \quad M' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix}$$

Prove that M x M' = $\begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}$ **[15 Marks]**

B. The DES algorithm combines two bit strings by applying the XOR operator on each pair of corresponding bits. Compute the 6-bit string that results from X-Oring 100111 and 110101 **[5 Marks]**

[QUESTION 4]

A. Your junior course mate asks you to help him decode the message **COHOBRGYRRYRITAPASHVTPFEE** he has just received from their CYS 110 lecturer. Use transposition cipher to decode and give him the answer **[5 Marks]**

B. Using the RSA encryption algorithm, let p = 3 and q =5. Then n = 15 and m = 8. Let e = 11. **[15 Marks]**
   i. Compute d.
   ii. Find the encoded text for CYBER CRIME
   iii. Decode your answer to part (ii) to retrieve the CYBER CRIME text.

[QUESTION 5]

A. You receive a message "**K, R, K, C, Q**" that was sent using the RSA public encryption key (21, 5). Decode this to find the original numeric and text message. **[10 Marks]**
B. Compare and contrast between Blowfish, Twofish and Serpent ciphers. **[5 Marks]**
C. The MD5 hash algorithm of Ron Rivest is in wide use today. Give the four steps involved in creating the 128 bit hush. **[5 Marks]**

[QUESTION 6]

A. You receive a message "14" that was sent using the RSA public encryption key (21, 5). Decode this to find the original numeric message. **[10 Marks]**
B. If **DREA** is the Key, use columnar transposition to decrypt the message **SEAZITFQIMRITIOU** **[10 Marks]**

[QUESTION 7]

A. State and explain any five active attacks that can be conducted by a hacker and cause a compromise on the confidentiality of the clear message m. **[10 Marks]**
B. Explain the main differences between RC4 and RC5 stating their advantages and disadvantages **[5 Marks]**
C. Define Authentication and hence differentiate between endpoint authentication and Message Authentication by giving appropriate examples. **[5 Marks]**

The End
The Future Is In Your Hands

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 (NETWORK SECURITY) PRACTICAL EXAMS

OCTOBER 2023

Do not turn this page until you are told to do so

This Question paper contains 2 Questions, attempt both of them.

Save your work with your ID and Question Number in a Single folder.

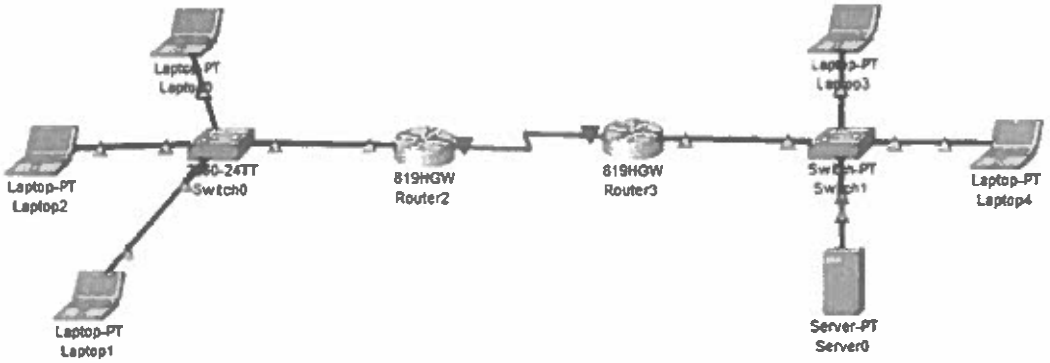
The folder should be named using your student ID

Time allowed is **1 h 30 Minutes** only.

No calculators are allowed in the exam

[QUESTION 1]

A. The bank of Zambia Network between Lusaka and Ndola offices is shown below. The Ndola office has an accounts server for the accounts department. It then has the HR and Operations department. Each of these departments has 10, 7 and 8 hosts respectively. The Lusaka office has the Admin, Finance and Security departments with 16, 21 and 17 hosts respectively. If the IP Address is **192.168.50.0/24**, use VLSM to subnet the network and show the following **[9 Marks]**
   I. The subnetwork Addresses
   II. The valid host addresses for each subnet
   III. The broadcast addresses
B. Configure the entire network with OSPF routing protocol so that the entire network can communicate. **[6 Marks]**
C. Use an appropriate access list to block all the departments from accessing the accounts server apart from the Admin and Finance department. **[5 Marks]**

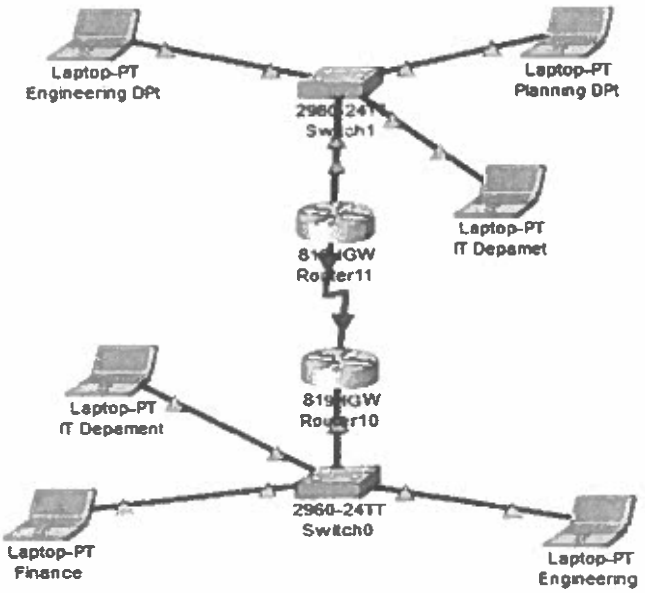


[QUESTION 2]

Chinsali Municipal Council has two offices one in New Town and the other one in old Boma. The IT department has just designed their internetwork as shown below. The IT department itself has 16 hosts, 4 at old Boma office and 12 at New Town. Planning department has 10 hosts all located at New Town office, finance deparment has 5 all located in New Town and finally the Engineering department has 14 hosts with 7 hosts at old Boma and the other 7 at New Town Office. The two offices are connected via a WAN link. As a new Network Administrator you have received the IP Address as **192.168.60.0 255.255.255.0** from ZAMREN your ISP.

A. Subnet the internetwork using VLSM **[5 Marks]**
B. Create a VLAN for each department **[8 Marks]**
C. Configure the internetwork with the RIP Version 2 Routing protocol **[4 Marks]**

D. Using an appropriate access list, configure a fire wall that will block all IP traffic from engineering and planning from going to the finance department. **[3 Marks]**



The End

The future is in your hands

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 THEORY EXAM

OCTOBER 2023

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 5 Questions, attempt any three.

All questions carry equal marks

Start each question on a new page.

Time allowed is **1 h 30 Minutes** hours only

Calculators are allowed in the exam

[Question 1]

A. Differentiate between an attack and a vulnerability **[5 Marks]**

B. Anomaly based and signature based IDSs used to detect a wide range of cyber-attacks. Explain how each one them works describing their differences. **[5 Marks]**

C. List and explain the three types of firewalls that can be used in the network to improve network security **[5 Marks]**

D. Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures. Name two reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. **[5 Marks]**

[Question 2]

A. What do the following abbreviations stand for? **[10 Marks]**

i. ISP
ii. ISO
iii. SLA
iv. OSI
v. IOS

B. A virus attacks a single user's computer and within one hour embeds itself in 60 e-mail attachment files sent out to other users. By the end of the hour, 25% of these have been opened and have infected their host machines. If this process continues, how many machines will be infected at the end of 5 hours? Can you find a formula for the number of machines infected after N hours? **[5 Marks]**

C. What is the difference between a virus and a worm as far as network security is concerned? **[5 Marks]**

[QUESTION 3]

A. Alice intends to send a message **m** to Bob but wants to make sure that the **message** has **integrity** and is both **authenticated** and **confidential** before sending it. Explain how she can use symmetric key, public key infrastructure and hush functions like SHA-1 to achieve the above stated goals. Use appropriate diagrams to explain your answer. **[15 Marks]**

B. What is a Message Authentication Code (**MAC**) and how is it created? **[2.5 Marks]**

C. What does the **PGP** abbreviation in the PGP protocol stand for and what is used for? **[2.5 Marks]**

[Question 4]

A. What do the initials SAD and SPD stand for in an IPsec Virtual Private Network? Hence state the difference between the two. **[4 Marks]**

B. How is an IPv4 datagram converted to an IPsec datagram by the IPsec like a router entity before transmission over the public network? Explain with the use of a diagram. **[8 Marks]**

C. Bank of Zambia has two branches, one in Lusaka and the Ndola office. The Lusaka (HQs) office has 23 hosts and one router and the Ndola (branch) office has one router and 12 hosts. If the institution is using VPN to communicate over the unsecured public network. How many SAs will be in the SAD If the director finance in Lusaka is communicating to 2 separate people at the Ndola Office? Explain your answer. **[3 Marks]**

D. Using appropriate diagrams, explain how you can secure a wireless network using IEEE 802.11i framework. **[5 Marks]**

[QUESTION 5]

A. What is end point authentications? Authentication protocol ***ap*2.0** requires that the two parties communicating have IP addresses. Explain what sort of attack can be used on ***ap*2.0** to cause a failure scenario. **[5 Marks]**

B. A onetime password is an example of a **nonce** used in ***ap*4.0**. Explain how the two parties, say Alice and bob, would use a nonce to authenticate each other. **[10 Marks]**

C. Explain the application protocol ***ap*3.0** and its failure scenario. **[5 marks]**

The End

The Future Is In Your Hands

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 110 TEST 3

FRIDAY 21ST JUNE 2024

TIME: 08:00HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 5 Questions, **attempt ALL questions**.

All questions carry equal marks.

Write your answers clearly

Time allowed is 2 hours only

Only calculators are allowed in the Exam room.

[QUESTION 1]

A. In your opinion, which one is the most important goal from amongst the goals of network security? Convincingly articulate your argument. [3]

B. Using AES algorithm, encode the following hexadecimal message sent using Rinjndael Algorithm. The S-Box, Round Key, initial state array and Predefined matrix are given below. Clearly show the four steps in the first round to get the final sate array in Round one. The S-box, predefined key, initial state array and the round key are given on the last page. [37]

[Total 40 Marks]

[QUESTION 2]

A. Using the RSA encryption algorithm, pick p = 5 and q = 7. Find a set of encryption/decryption keys e and d. [4]

B. Using the keys that you have found encrypt the word **LOANS BOARD** assuming that the alphabet is between 1 and 26. [8]

C. Use the decryption key you obtained above, decrypt the cipher text **ROWPHAWI.** **[8]**

[QUESTION 3]

A. The centurion who was supposed to inform you of s was killed en route, but you have received the message **VGFRVUREVCNFFBEVSNVY** in a Caesar cipher. Find the value of s and decode the message. Hint: *Use brute force* [5]

B. Your junior course mate asks you to help him decode the message **YANAHSCGAERHPHOSAOTYTINNRRNETTIOCBETE** he has just received from their CYS 110 lecturer. Use columnar transposition cipher to decode and give him the answer using the key **QUARTZ** [5]

C. Using a Caesars cipher with S = 3 and S = 9, Encrypt the message **ACCURACY IS CARDINAL** using a C1C2C2C1C2 sequence [5]

D. The three blocks of hexadecimal numbers **24 45 37, 64 44 A1** and **3B 22 09** need to be hushed in order to get a check sum so that the information they contain maintains its integrity. Calculate the checksum using hexadecimal addition. [5]

[QUESTION 4]

A. You receive a message that was encoded using a block encoding scheme with the encoding matrix, Decode the cipher text MXOSHI [10]

$$M = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \quad M' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix}$$

B. Prove that M x M' = $\begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}$ **[5]**

C. Using the RSA encryption algorithm, let p = 3 and q =5. Then n = 15 and m = 8. Find the encryption and decryption keys. [5]

ALL THE BEST WISHES

THE END

S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Predefined Key

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Initial State Array

EA	04	65	85
83	45	5D	96
56	33	98	B0
F0	2D	AD	C5

Round Key

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

KAPASA MAKASA UNIVERSITY
PAST EXAMINATION PAPERS
2023

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY
SECOND YEAR CYS

COURSE CODES:

CYS 215

CYS 220

CYS 230

CYS 210

CYS 212

CYS 22

CYS 211

KAPASA MAKASA UNIVERSITY

BSc. Degree in Cybersecurity

CYS 211: SOCIAL NETWORK ANALYSIS

OCTOBER 2023 SESSIONAL EXAM

DURATION: 3HRS

INSTRUCTIONS:

1. This paper has two sections: **Section A and B**
2. Section A is Compulsory and has two (2) questions.
3. Answer any three (3) questions from section B.
4. All questions carry equal marks
5. Write your answers clearly

SECTION A:

QUESTION 1

Using the figure given below:

	Actor	*Lines near:*
n_1	Allison	Ross, Sarah
n_2	Drew	Eliot
n_3	Eliot	Drew
n_4	Keith	Ross, Sarah
n_5	Ross	Allison, Keith, Sarah
n_6	Sarah	Allison, Keith, Ross

a) Draw the Social Matrix represented by the figure above. **[2 Marks]**

b) List all the geodesic distances for each node in the graph. **[10 Marks]**

c) Write a C++ program which will be able to compute the number of lines using the social matrix generated in b). **[8 Marks]**

Total Marks: 20

QUESTION 2

a) Define the term Social Network Analysis? Give one example of a situation in which a social network can be modelled and state which information can be obtained. **[5 Marks]**

b) Define the following Social Network Analysis terms: Two mode network, digraph, trees, bipartite graph, Nodal out-degree, Walks, trails, paths, geodesic distance, diameter, connected graph. **[10 Marks]**

c) Mention five (5) techniques that can be used to collect Social Networks data. **[5 Marks]**

Total Marks: 20

SECTION B:

QUESTION 3

a) Give two (2) definitions of a Random Network according to Erdös and Renyi, and Gilbert. **[4 Marks]**

b) Define how a Breadth First Search algorithm is used to traverse a graph. **[4 Marks]**

c) Using the Breadth First Search algorithm, show clearly how the graph below will be traversed at each stage. You should show the status of the graph and the queue at each stage of the search. **[12 Marks]**

Total Marks: 20

QUESTION 4

a) Define each of the following Network Centrality terms: Closeness, Betweeness and Eigenvector. **[6 Marks]**

b) What is a community with regards to graph theory? **[2 Marks]**

c) Give five (5) reasons why community detection is important in graph theory. **[5 Marks]**

d) Given the graph below: clearly show how it will be traversed using Breadth First Search algorithm. You should write the resulting sequence of letters. **[7 Marks]**

Total Marks: 20

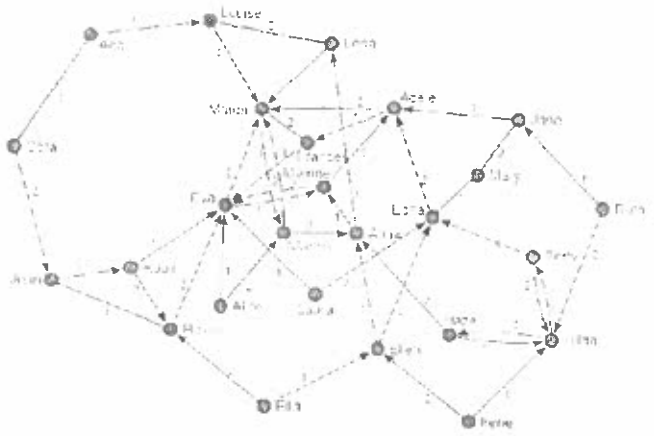
QUESTION 5

a) Briefly describe how the six-degrees or small world concept with regards to social network analysis. **[4 Marks]**

b) On Twitter and facebook, how is a node defined and two properties that can be recorded for that specific node. **[4 Marks]**

c) Briefly explain how the following Social network analysis terms are used to analyse social media networks such as Facebook and Twitter: in-degree, out-degree. **[4 Marks]**

d) Using the Sociogram given below, identify the most popular actor and least popular actors. **[8 Marks]**



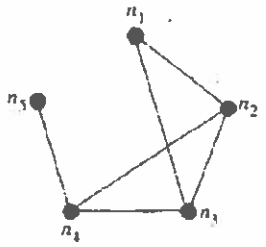
Total Marks: 20

QUESTION 6

a) Define a graph in relation to social network analysis? Give three (3) reasons why graph theory is useful in Social Network Analysis. **[5 Marks]**

b) Briefly describe the difference between structural and composition variables in relation to Social Network Analysis. **[4 Marks]**

c) Using the graph below, calculate the geodesic distance of each node and determine the diameter of the graph. **[9 Marks]**



Total Marks: 20

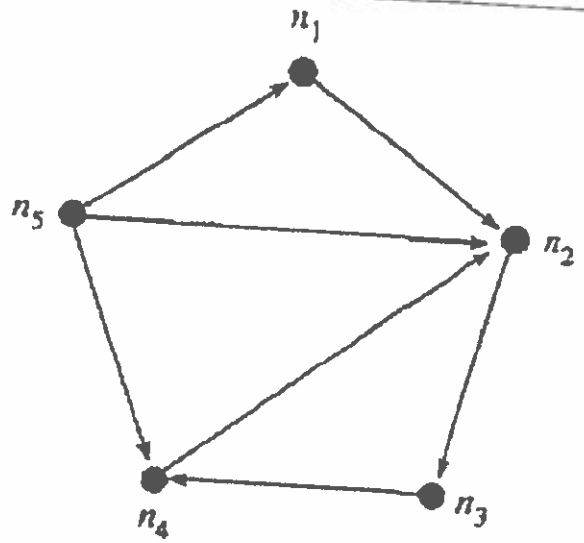
QUESTION 7

a) Describe in detail how social Network Analysis Concepts can be used to analyse computer services that were compromised by various malicious programs. **[10 Marks]**

b) Using the directed graph below, show the sequence of routes for a : Directed walk, Directed path, semipath, Cycle, and Semicycle **[10 Marks]**

Total Marks: 20

END OF PAPER



KAPASA MAKASA UNIVERSITY

DEPARTMENT OF EDUCATION AND ODL.

2023 FINAL CY22 EXAMINATION

COMMUNICATION SKILLS

INSTRUCTIONS

1. TIME ALLOWED is only THREE (3) HOURS
2. This paper contains 7 questions on 4 pages; you are required to attempt SEVEN (7) of them, including **QUESTION ONE which is compulsory.**
3. Begin each question on a new page.
4. All answers should be couched in Standard English
5. Ensure that you write your **SIN,** on your answer booklet.

Question One (Compulsory)

***INSTRUCTIONS*: Change the following conversation into minutes**

Chanda: "Ah, Mr. Secretary, good day to you; is everyone here?"

Sililo: "Let me see, Mr. Mulenga, the new Catering Officer is here, Miss Zulu from accounts. Mr. Banda from Tailing plant, but I can't see Mr. Zimba from stores and you remember that Mrs. Phiri gave her apologies in advance at the last meeting as she is on leave; so Bookshop will not be represented."

Chanda: "I don't think that we will wait for Zimba, we have a quorum, so let's begin. I call this meeting to order. There is no need to read the summons concerning the meeting and you all have the minutes of the last meeting. Any amendments?

Zulu: "Yes, Mr. Chairman, I have been left out of the list of those in attendance but you can see from item 6 that I was present because I reported on the availability of new cups from Shoprite".

Sililo: "Apologies Mary, I remember now that you came a little bit late so you didn't sign the attendance".

Chanda: Let us not make that mistake again. Her work-fellows know that she gets time off to attend these meetings and if she takes the time off and then doesn't attend the meetings, she could be in trouble with them. Any more corrections? No? Good, I will sign the minutes then. Now, any matters arising.....Mr. Secretary?"

Sililo: "Yes, Mr. Banda and Zimba were supposed to get their heads together to work out different tea break times for their departments, so that they don't all try to get in here together."

Chanda: "Mr. Banda?"

Banda: "Well we can't agree. Our work-fellows all want to be here first but feel our work is harder than Bookshop so we need the break earlier."

Chanda: "So, we'll have to wait for Zimba. Anything else?"

Sililo: "Yes, the matter of Saturday opening."

Chanda: "Yes, I've talked to the General Manager and he doesn't think it's worth opening the canteen just for a morning tea break if we aren't going to provide lunch on the same day. Ah Mr. Zimba..... Come in, we started without you".

Zimba: "Sorry to be late. One book went missing and you know our rule, no one leaves till the book is found."

Sililo: Mr. Zimba, what about the morning tea break times?"

Zimba: "It's OK my chaps have given in. They will take the later time if I can get assurance that the tea and bread will-not run out."

Chanda: "Mr. Mulenga ..... I do apologize, I should have properly welcomed you to this committee. To tell the truth, I have seen so much of you since you joined us three weeks ago that I forgot that you have not yet attended one of these meetings. You know everyone here, I suppose.....

Mulenga: "Yes thank you Sir, and as to there being enough leftovers for the late comers, don't you worry about that even though I am busy making up that report you asked to be ready for next month's meeting on the refrigeration needs."

Chanda: "Fine, we'll put the new time into operation on Monday if that gives the Secretary enough time to inform all the people."

Sililo: "Not really Mr. Chairman, this is Friday afternoon already. Can we agree to start the new system on Tuesday? That will give me time to inform everyone, otherwise we might get into some confusion."

Chanda: "Right, we'll start on Tuesday. Bookshop 09.45 to 10.05 hours Stores 10.10 to 10.30 hours and the rest after that."

Zulu: "Good Lord! Look at the time. I've a meeting with the Company Secretary in five minutes. Is there any pressing business or shall we let Mr. Mulenga find his way around for next month's meeting before we start chasing him?"

Sililo: "There is no news about our application for a bar licence, so the question of opening the canteen in the evening for should start thinking about the Christmas party but that can wait until next month."

Chanda: "So can we adjourn?"

Chanda: "Meeting adjourned till next month, same place, same time."

You look at your watch, its 16.00 hours.

Question Two

After your graduation you have seen an advert by the company secretary of ZAMTEL that he is recruiting fresh cyber graduates.

Apply for the job.

Question Three: Study the Table Below

PROGRAMME									
Agro Forestry		9	3	38	48	52	21	14	3
Fisheries And Aquaculture		9	1	29	18	66	14	31	9
Animal Science		8	2	17	18	37	12	25	6
Wood Science And Technology		10	0	18	3	37	12	25	6
Education		7	7	15	19	23	15	12	1
Forestry		11	2	14	2	16	2	4	0
		M	F	M	F	M	F	M	F
		1st Class	1st Class	2nd Class	2nd Class	Pass	Pass	Failure	Failure

PERFORMANCE OF UNIVERSITY STUDENTS IN VARIOUS FACULTIES

From the observations of the table above, give answers to the following questions.

a. Which programme has the greatest enrolment of male students?
b. Which programme has the least enrolment of students?
c. Total enrolment of students in the faculty of education.
d. Total enrolment of female students in Education.
e. Total enrolment of male students in Fisheries and Aquaculture.
f. Which programme has the greatest number of passes?
g. Which programme has the greatest number of failure?
h. Which programme has the least number of failures?
i. The number of students who achieved a pass or better in Agro Forestry.
j. The number of female students who achieved a pass or better in wood Science and Technology.

k. The number of male students who achieved a pass or better in Animal Science. Which programme has the greatest number of 1st class standing?
l. Which programme has the greatest number of 2nd class standing?

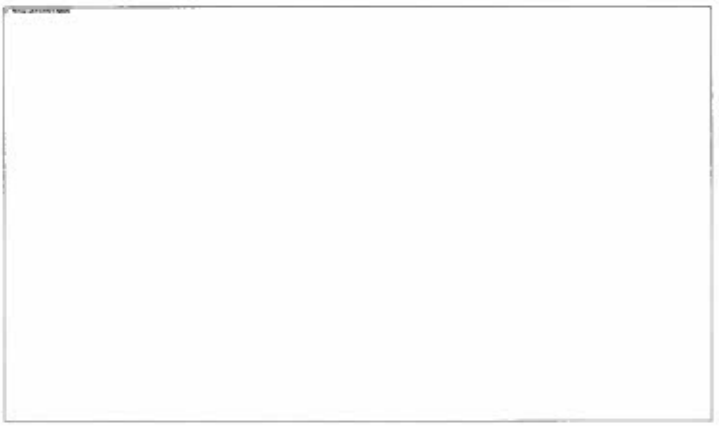
Question Four: Write a 600 word essay on VARIOUS TYPES OF PLAGIARISM

QUESTION Five:

Change the following sketched data in to well **NUMBERED** outline notes

History of Mr. Kapasa Makasa

Kapasa Makasa University is named after the late author, freedom fighter and politician, Mr. Speedwell Robert Makasa, who died on 2nd February 2007. Mr. Makasa renounced the two foreign forenames and took on Kapasa as a first name before his death.



Public Service History and Curriculum Vitae of the late Mr. Kapasa Makasa

- **29/01/1922** - Date of birth
- **1943-1953** - Teaching at Mufulira, Choma and Lubwa for 6 years
- **1945** - Mine Clerk (Wusakile Compound Office), Nkana Mine
- **1947** - Elected Committee Member of the Federation of African Welfare Societies under the Chinsali Branch
- - Elected Church Elder in the Church of Scotland (now United Church of Zambia
- **1950-1951** - Chairperson of the African Congress, Chinsali Branch
- **1951-1952** - District Organising Secretary of African Congress, Chinsali Branch
- - Member of Teachers Association – Chinsali Branch
- - Took the Government Efficiency Bar examination – Northern Rhodesia (1st Class)
- **1953-1955** - Provincial President of African National Congress of Northern Rhodesia
- **1955-1956** - Imprisoned for one and half years for conducting a boycott of Thomas & Company stores
- **1959-1960** - Restricted to Solwezi district under state of emergency; Chairperson for Advisory Committee for those restricted

- **1960** - Divisional President for Luapula Province under the Zambia African National Congress after restrictions
- **1961-1962** - UNIP Representative in Tanganyika.
- - Chairperson of group of freedom fighters of PAFMECA.
- - Attended Youth Seminar in Pakistan
- **1963** - Oxford (UK) – Public administration short course
- **1963** - UNIP Regional Secretary, Katete/Chadiza region
- - Member of Parliament – Chinsali North
- - Parliamentary Secretary – Ministry of Agriculture
- **1964-1967** - Resident Minister for Northern Province
- **1967** - Minister of State – Ministry of Foreign Affairs
- **1968** - Cabinet Minister for North-western Province
- **1968-1969** - Ambassador to Ethiopia
- **1970-1972** - Cabinet Minister – Luapula Province
- **1972-1975** - High Commissioner – Tanzania
- - Ambassador – Rwanda, Burundi & Madagascar
- **1975** - High Commissioner - Kenya
- **1978** - Member of Central Committee – Lusaka Province
- **1979** - Chairperson – Rural Development Committee of the Sub-Committee of UNIP Central Committee
- **1980** - Patron of Lubwa Mission Church; Member CUSA for Lusaka Branch
- **1983** - Chairperson – Zambia Agricultural Development Bank
- **1987-1991** - Chairperson – SIDO
- - Chairperson – Lima Bank Board of Directors
- **1991** - Retired from active politics

Question Six: Using the structure of a formal definition define A COMPUTER AND A BALLPEN SEPARATELY

Question Seven: Your friend has been invited to attend a job interview. Write brief notes to advise him on the following;

a. What to do before the day of THE INTERVIEW?
b. What to do on the day of the INTERVIEW?

END OF THE EXAM!

God bless you.

KAPASA MAKASA UNIVERSITY

INFORMATION AND COMMUNICATIONS TECHNOLOGY

CYS 212

CYBER SECURTY PENETRATION TESTING

FINAL EXAMINATION

OCTOBER 2023

DURATION 4 HOURS

There are SIX questions in this paper

Candidates should answer ANY FIVE QUESTIONS in this PAPER

This paper does not in any way attempt to cause harm or come in conflict with other organizations resources in this paper. The paper is purely a drive-by for educational purposes only.

QUESTION 1

What is information Gathering 2 Marks

There are several available tools such as nmap; Zenmap etc that you can use to conduct information gathering techniques on targets

i) Using nmap command: nmap –v
Conduct an information gathering technique on website kmu noting all open ports as follows:

a) www.kmu.ac.zm
b) www.zipar.org

(Paste your results on soft answer sheet) **6 Marks**

Compare the results on the two targets. What is your observation in terms of results? What does it tell you as a hacker?

2 Marks

ii) Now perform a deep packet **intense port scan** using **Zenmap** in promiscuous mode scan for the three above targets in (i)

a) discover clearly both **tcp** and **udp** ports
b) Paste output of all open ports
c) Paste output of all closed ports

(Paste your results on soft answer sheet) **4 Marks**

iii) In your service enumeration process, on target (b) perform a **banner grabbing** for all of the discovered open service ports. **List also services one by one** along with its **port & service**

(Paste actual banner output for each port)

iv) From your information, what service is running on port 53?
v) What advise can you give KMU for exposing port 53

6 Marks

Total 20 Marks

This paper does not in any way attempt to cause harm or come in conflict with other organizations online resources. The paper is purely a drive-by for educational purposes only.

QUESTION 2

(If you had earlier downloaded, an index file for any site delete it before you attempt this question to avoid conflicts)

Your FOLLOW UP stage in your penetration hacking is to find out what name servers exist in the organization. Out of many attacking options, DNS is one of them on the particular target: kmu.ac.zm; zipar.org.zm & mukuba.edu.zm

a) Perform a **dns enumeration** for the IPs and attempt **dns zone transfer** on the following target domains:

10 marks

b) (paste actual output)

c) Run a command (on domain names in question) and **pipe the result** into a text file call it **enum_gx.txt** (gx your initials **3 marks**
(paste output)

d) List the names of **domain controllers** server names responsible for internal network addressing and their corresponding IP Address

7 marks

(paste actual output)

Total 20 Marks

QUESTION 3

On the target below,

www.kmu.ac.zm
www.zipar.org

a) Download an index file from one of the sites and analysis it 2 Marks
(Paste output)

b) Whip-up a clean bash script to identify your targets sites subdomains involved 9 Marks
(Paste output)

c) Whip-up another bash script to perform a ping sweeper to discover their live servers behind those subdomains; services and paste the scan results 9 Marks

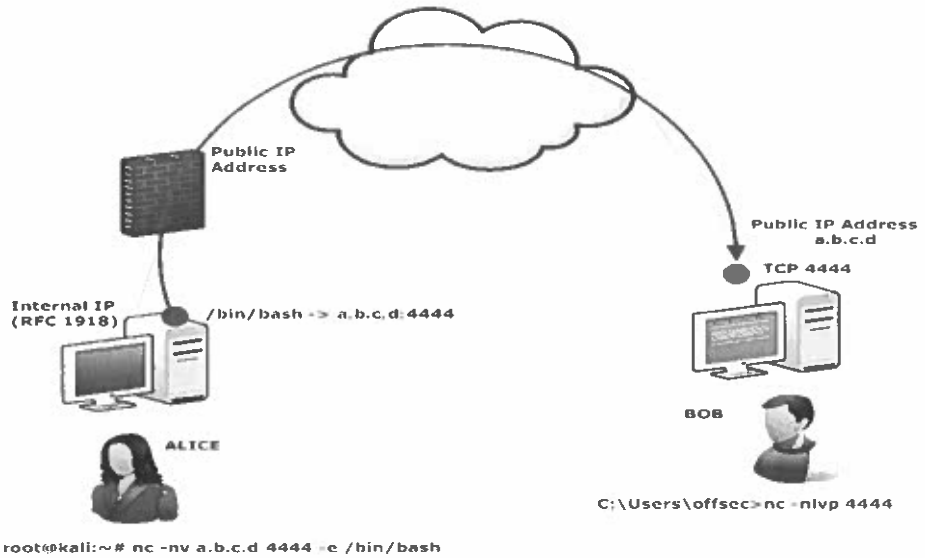
Total 20 Marks

This paper does not in any way attempt to cause harm or come in conflict with other organizations online resources. The paper is purely a drive-by for educational purposes only.

QUESTION 4 Required for this question - only explanation

a) What are the main goals and reasons for conducting a penetration testing for your organisation as a cyber-security professional - show benefits

8 Marks



b) The diagram shows how you as a hacker can use various tools such as netcat to gain access to a vulnerable computer; gain control remotely, and perform remote code execution. In your lab exercise, you performed this practice with netcat as a malicious tool.

Explain clearly how you were able to gain access to a remote computer and ran appropriate commands, (where necessary show those commands you executed in respective computers local and remote)

8 Marks

How you transferred malicious files to exploit a remote computer

4 Marks

Total 20 Marks

QUESTION 5

(If you had earlier downloaded, an index file for any site delete it before you attempt this question to avoid conflicts)

Given a domain unza below, give attention and explore the details of the website its index file

(Paste output, just any section of index content)

1. Identify the subdomain under the Unza domain

   (Paste output of the extracted filtered)

2. Pipe the output to a file give it a name **unza_xg.txt** (where xg are initials of your first and last names

   (Paste output; content of file)

   -Browse to check if the file exist in your Kali and
   -Look over the file.

3. You are required to quickly whip-up a born-again **Bash Script** below to help you automatically generate the **corresponding IP Addresses** to the Identified subdomains. Bash script name should be: **umatchip.sh**

```
#!/bin/bash
for url in $ (cat unza_gx.txt); do
host $url
done
```

Save the script;
browse to check it exists;
give it executable permissions and ;
execute it

Paste output corresponding ips to subdomains

4. Write an appropriate bash script to echo filtered and clean range from **3 to 250** of IPs range to be echoed in (4.) the script name should be : **echo_unzaip.sh**

   Paste output a section of echoed IPs

5. Write an appropriate bash script, a ping sweeper to ping the IP range from **10 to 250**. The script name should be : **ping_unzaip.sh**

Total 20 Marks

QUESTION 6

(If you had earlier downloaded, an index file for any site delete it before you attempt this question to avoid conflicts)

You intended to perform a deep packet or **intense port scan** using **Zenmap** in promiscuous mode to scan for an organization website www.mukuba.edu.zm

a) Using www.mukuba.edu.zm as target, discover both **tcp** and **udp** ports

b) List or paste output of all open ports

c) List or past output of all closed ports

6 Marks

Given a domain above, give attention and explore the details of the index

Paste output, just any section of index content

6. Identify the subdomain under the mukuba domain

Paste output of the extracted filtered

7. Pipe the output to a file give it a name **mmukuba_xg.txt** (where xg are initials of your first and last names

Paste output; content of file

-Browse to check if the file exist in your Kali and **4 Marks**
-Look over the file.

8. You are required to quickly whip-up or write a given **Bash Script** below to help you automatically generate the **corresponding IP Addresses** to the Identified subdomains.

Bash script name should be: **mmatchip.sh**

```
#!/bin/bash
for url in $ (cat mmukuba_gx.txt); do
host $url
done
```

Save the script;

browse to check it exists;
give it executable permissions and ;
execute it

6 Marks

Paste output corresponding ips to subdomains

9. Write an appropriate bash script to echo filtered and clean range from 1 **to 250** of IPs range to be echoed in (4.) the script name should be : **echo_mmukubaip.sh**

Paste output a section of echoed IPs

10. Write an appropriate bash shebang script as a ping sweeper to ping the IP range from **1 to 250**. The script name should be : **ping_mmukubaip.sh**

4 Marks

Total 20 Marks

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES AND EDUCATION

2023 SESSIONAL EXAMINATION

CYS 210 – CYBER THREATS, INTELLIGENCE AND RESPONSE

INSTRUCTIONS

(1) Time allowed is **Three (3) hours**.

(2) There are two sections in this paper, **SECTION A** and **B.** Answer **ALL** Questions in **Section A** and **Any THREE** from **Section B**.

(3) Each question carries **20 Marks**.

Ecclesiastes 9 vs 10-11

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO

Section A: Compulsory Questions

Question one

a) Explain why it is necessary to protect against Cyber threats **[5 Marks]**

b) Carefully study the attack below and explain how it is perpetrated and the measures that can be put in place mitigate this kind of attack. **[9 Marks]**

c) A good place to start to understand how to protect your organization from cyber threats is the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (NIST Cybersecurity Framework). Explain the process of Cyber Threat Intelligence. **[6 Marks]**

Question Two

It is Wednesday, August 30, 2023 at 10:00 AM Central African Time. You are a security analyst for a Zambia National Commercial Bank. You receive an alert from your intrusion detection system (IDS) that there has been a suspicious login attempt to one of the company's servers. The login attempt was made from an IP address that is not associated with any known employee or vendor who happens to know your organization very well.

a) As a security expert, you are required to carry a thorough investigation into the login attempt and identify the attacker. **[3 Marks]**

b) Once the attacker has been identified, provide a detailed report to management on how you managed to identify the threat and respond to it. **[7 Marks]**

c) Provide a detailed analysis of the problem and the measures put in place to avoid future occurrences of such incidents. **[5 Marks]**

d) What emerging technologies or trends, such as the Internet of Things (IoT) or 5G, pose unique challenges in terms of cyber threats and intelligence? How can organizations prepare for these new threats. **[5 marks]**

Section B: Answer any three Questions

Question Three

a) Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff. The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives. Identify the type of threat intelligence information that Tracy could use to achieve her objectives. **[10 Marks]**

b) An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on. Discuss the sources that will help the analyst to collect the required intelligence information needed. **[10 Marks]**

Question Four

In the recent past some hackers introduced malware onto National Pensions Scheme Authority (NAPSA) systems, stealing substantial amounts of data and causing disruptions for the authority's clients. Describe the steps you would take to investigate the incident, gather threat intelligence, and implement a response plan to prevent similar breaches in the future at NAPSA. **[20 Marks]]**

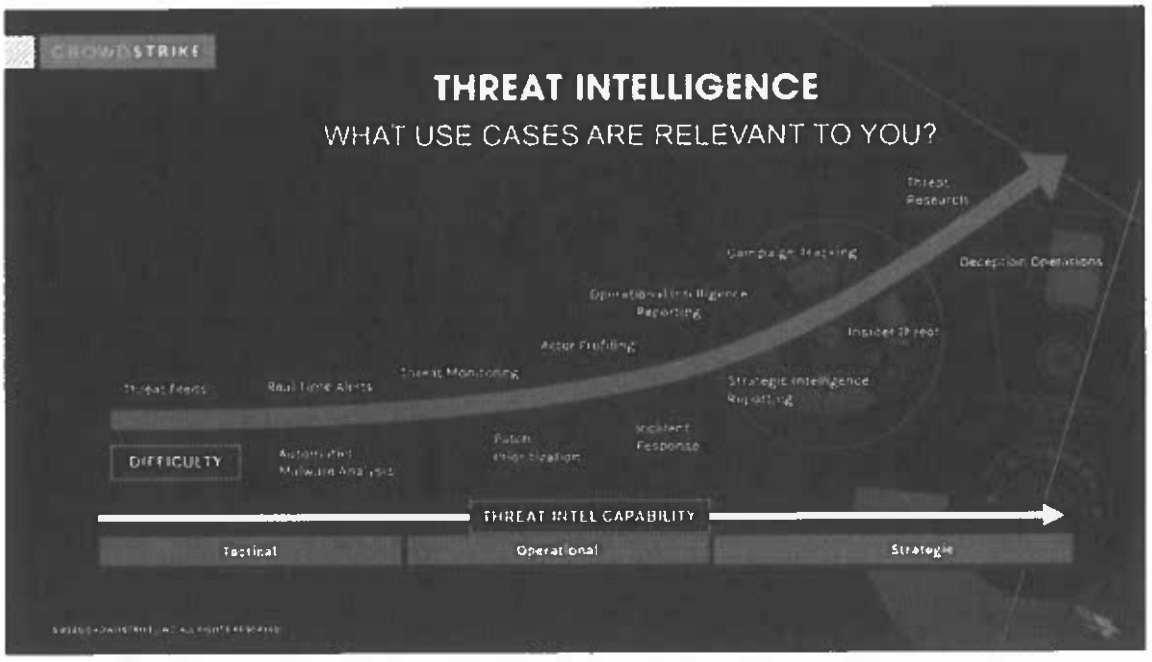
Question Five

a) An energy utility company suspects a cyber threat targeting its power grid infrastructure. As a cybersecurity expert, outline the process of threat hunting and intelligence gathering you would employ to confirm the presence of malicious activities and mitigate potential damages. **[10 Marks]**

b) You are part of a Security Operations Center (SOC) team for a financial institution. One of your colleagues has reported a suspicious incident involving an employee's compromised account. Explain the actions you would take to analyze the incident, use threat intelligence, and collaborate with other teams to contain and remediate the threat. **[10 Marks]**

Question Six

a) Consider the threat intelligence use case diagram below:



Explain the threat intelligence capabilities as occurs at all the three levels of the use case (Tactical, operational and strategic). **[6 Marks]**

b) List the some general skill characteristics that many government intelligence analysis functions have used for years and are commonly agreed within the industry. **[10 Marks]**

c) Briefly explain the reasons why Threat intelligence is important. **[4 Marks]**

KAPASA MAKASA UNIVERSITY

DEPARTMENT OF ICT

CYS 230
Cybercrime Investigation Forensic I

2023 Early Session Examination

(2 hour 00 minutes)
(60 marks)

INSTRUCTIONS:

- They are two sections in this paper, answer them all in the answer booklet provided.
- Section A, choose, and write the best answer
- Section B, provide a brief statement as a response to the questions therein
- The use of calculators or any other computerized device (eg a phone) is not allowed.

Section A Multiple Choice Questions, Write the best answer in the grid (20 Marks)

Questions:

1. Which of the following techniques are used during computer forensics investigations?
   A. Cross-drive analysis
   B. Deleted files
   C. Live analysis
   D. All of the above
2. You are suppose to maintain three types of records. Which answer is not a record?
   A. Chain of custody
   B. Document your actions
   C. Documentation of the crime scene
   D. Searching the crime scene
3. Volatile data in a computer system resides in?
   A. Cache
   B. Hard drive
   C. RAM
   D. A and C
4. Deleted files Recovery is a common technique used in computer forensics in the recovery of deleted files as evidence. Which statement below is correct.
   A. False, as the evidence can not be used in court
   B. It is impossible to recover deleted files
   C. True, although the evidence can not be used in court
   D. True, as the evidence can be used in court
5. The investigator has to take the following precautions while collecting evidence (which option is incorrect):
   A. before arrival
   B. photograph the equipment with it serial number, model number & writing schemes.
   C. seeks Magistrates permission before investigating a cognizable offence labelling the evidence
   D. videotaping the scene, to document the system configuration and the initial condition of the site
6. Access or attempt to access by any unauthorized person, a protected computer system as notified by the Government in the Official Gazette where punishment may extend up to 10 years:
   A. Cognizable, Bailable
   B. Cognizable, Non-Bailable
   C. Non- Cognizable, Non-Bailable
   D. Non-Cognizable, Bailable
7. When to start investigation:
   A. After receiving authority from Inspector of Police
   B. After receiving permission from Cyber Crime Division
   C. As soon as non-cognizable offence is brought to the notice of Police
   D. In case of cognizable offence after lodging of the First Incident Responder (FIR)
8. Prosecution has to give copies of:
   A. All electronic records relied upon by the prosecution to the Accused
   B. Non-electronic records involved in the case to the Accused
   C. Only certain electronic documents to the Accused
   D. Only those copies of the electronic records which are contained in an external hard disk, pen drives, CD; flash drives, etc.

9. What is the full form of SOP in cell device forensic?
    A. Safety Operational Procedure
    B. Set Operational Procedure
    C. Standard of Preservation
    D. Standard Operating Procedure
10. What is the use of a write blocker in mobile forensic?
    A. To ensure the safety of mobile evidence
    B. To disable the wireless communication to the device
    C. To block all the white hat hackers from assessing mobile devices
    D. To prevents any changes of a driver information
11. CDRs in mobile forensic stands for
    A. Call Data Records
    B. Call Detail Records
    C. Compact Disk Readers
    D. Compact Disk Rewritable
12. What is used during computer forensics investigations?
    A. Deleted files
    B. Live analysis
    C. Reverse steganography
    D. All of the above
13. Which of the following program is run to examine network traffic:
    A. Core dump
    B. Net dump
    C. Slack dump
    D. TCP dump
14. Which digital forensic software is commonly used for mobile device forensics?
    A. Autopsy
    B. Cellebrite
    C. EnCase
    D. Wireshark
15. Which digital forensic software is commonly used for network forensics?
    A. Autopsy
    B. Cellebrite
    C. EnCase
    D. Wireshark
16. Which of the following is NOT a category of digital evidence?
    A. Emails
    B. Eyewitness testimony
    C. Network logs
    D. Social media posts
17. What is the purpose of hash values in digital forensics?
    A. To analyze network traffic
    B. To encrypt digital evidence
    C. To recover deleted files
    D. To verify the integrity of digital evidence

18. A computer network spanned inside a building and operated under single administrative system is generally termed as
    A. PAN
    B. LAN
    C. WAN
    D. SAN
19. What name is given to a decoy that has network-accessible resources, and can be deployed in a network as surveillance and early-warning tools?
    A. Honeypot
    B. Honeynet
    C. Honeywall
    D. A decoy
20. Network forensics systems can be one of two kinds, one system, allows all packets passing through a certain traffic point to be captured and written to storage with analysis being done subsequently in batch mode. What do we refer to such a system as ?
    A. Stop, look and listen
    B. Catch-it-as-you-can
    C. Catch-it-as-you-see
    D. Stop, look and store

SECTION B (Answer using brief statements only) (40 Marks)

Compulsory Questions

1. Define and discuss what a cybercrime is. While giving at least two (2) examples of any common cybercrimes that go unpunished in Zambia. [4]
2. Describe and summarize the Cyber Security and Cyber Crimes Act, 2021 in less than 200 words. [5]
3. Cyber forensics involves thoroughly scientific activities for examination and analysis of digital evidence in such a way that the information can be used as evidence in a court of law. Mention any four [4] of those forensics' activities. [4]
4. Briefly describe and/or define the following cybersecurity threats: [10]
   a) Hacking *(2)*
   b) Keylogger *(2)*
   c) Botnet *(2)*
   d) Sextortion *(2)*
   e) DOS attack *(2)*
5. All security threats are intentional as they occur when intentionally triggered. And these security threats can be divided into the following categories: Interruption, Privacy-Breach, Integrity and Authenticity. Briefly explain what the following are: [4]
   a. Interruption
   b. Privacy-Breach
   c. Integrity
   d. Authenticity
6. In a court of law, how could one demonstrate that the image clone of a computer system is unaltered, not a true copy of the original, beyond any reasonable doubt. Briefly explain any two factors you would consider using for your defense. [4]
7. Mention any four areas where evidence on Application Layer of the OSI model can reside in when working with network forensics. [4]

Choose any one from the Question Below

8. What are the benefits of computer forensics and investigation? Mention any five (5) [5]
9. The cyber investigation processes applicable when working with digital evidence involve a process of assessing and analysing the scope and situation of the investigation and the action to be taken, acquiring, gathering, protecting, and preserving the data for the original evidence, analysing, examining and correlating the acquired the data of the digital evidence. Clearly elaborate the stages and/or of computer forensics investigation process. [5]
10. Many incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. List and explain any give of such considerations. [5]
11. Evidence preservation is the process of securely maintaining custody of property without altering or changing the contents of data that reside on devices and removable media. It is the first step in digital evidence recovery. As an incident officer, explain how you can preserve data at a cybercrime scene, clearly elaborating each stage of the process. [5]

KAPASA MAKASA UNIVERSITY

COMPUTER SCIENCE DEPARTMENT

ETHICAL HACKING

CYS 220

FINAL EXAM

Instructions

i. Time allowed: **3 hours**, Total Marks allocated to each question: **20 Marks**
ii. There **SIX Questions** in this Paper Answer **ANY FIVE** questions.
iii. The marks allocated on each question give a clue as to the depth of you answer.
iv. **Please, where appropriate, use diagrams and/or examples**

KAPASA MAKASA UNIVERSITY

DEPARTMENRT INFORMATION AND COMMUNICATION TECHNOLOGY

CYS 215 BIOMETRIC SECURITY

SESSIONAL EXAMINATIONS

Duration: **3 Hours** Total Marks allocated: **100**

Instructions

1. **There Six** questions in this paper Answer **ANY Five**
2. The marks allocated on each question give a clue as to the depth of you answer
3. Please, where appropriate, use diagrams and/or examples
4. There are **3 Pages** in this paper

QUESTION ONE

a) Explain the meaning of a term "Biometrics" [2 Marks]

b) Identify reasons you would cite in your recommendation of a biometric authentication system? [6 Marks]

c) What TWO challenges would you state as a precaution in your recommendation of the Biometric Authentication System [4 Marks]

d) What are some of the ethical and legal issues associated with biometric data collection and storage? [8 Marks]

QUESTION TWO

In the not-so-distant future, it is expected that most Applications are going to integrate biometrics for improved security. However, challenges have been anticipated.

a) Mention the Three (3) challenges associated with integrating biometric systems into existing infrastructure? [6 Marks]

b) A benchmark is a standard or criteria used for comparison to ascertain how best a measured or assessed object or concept is.
Explain the SEVEN (7) criteria for the effective biometric system [13 Marks]

QUESTION THREE

a) Explain FOUR (4) of the future trends in biometrics Applications [12 Marks]

b) How can biometric systems be made more secure? [3 Marks]

c) Identify and briefly explain the FIVE (5) criteria for generating biometrics templates [5 Marks]

QUESTION FOUR

a) Explain the architecture of a Biometric authentication System with a visual aid [12 Marks]

b) Show a contrast between voice recognition and speech recognition [2 Marks]

c) Discuss Three (3) Strength of Biometric authentication over traditional authentication [6 Marks]

QUESTION FIVE

a) State TWO (2) strength of Iris Recognition system over facial recognition System [4 Marks]

b) Biometrics algorithms are mathematical algorithms used in biometric systems to process, analyze, and compare biometric data to identify or verify an individual's identity.
Write brief notes on the following algorithms:
   a. Minutac based algorithm [5 Marks]
   b. Pattern based algorithm [5 Marks]

QUESTION SIX

a) Write brief notes on Cloud based biometrics [5 Marks]

b) Explain the term Invasiveness in relation to TWO biometric modalities that you know with examples. Also state how this is a challenge to Biometric adoption [6 Marks]

c) In a tabular format compare the THREE(3) Biometric modalities with examples [9 Marks]

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

FRAUD AND DETECTION TECHNOLOGIES

CYS 339

SESSIONAL EXAMINATION

DATE: 25-Oct-24 TIME: 14.00 - 17.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Seven (7) questions** in this paper. Attempt any **five (5).** Indicate on the Answer sheet your choice from the optional questions.
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets ( ) at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION 1

a) After your graduation, you started working as a cyber security officer at Zamnet and your boss tasked to write a report on the measures the bank can undertake to prevent fraud. Write a report, in point form, outlining five (5) the bank can take. (10 marks)

b) Explain four (4) white collar crimes in relation to fraud. (4 marks)

c) Using two (2) examples in each case, differentiate between internal and external threats to a fraud detection system. (6 marks)

[Total: 20 marks]

QUESTION 2

The Law provide a formal mechanism for the creation and maintenance of social order in complex societies. They define crime, whether a crime has been committed, whether a given person is guilty of the act, and the convicted offender's punishment. The level of "evilness" is the basis of crime. We can distinguish crimes from one another in terms of the length of punishment and place of confinement. This is called grading. Crimes are generally graded into three categories:

a) Felonies, (8 marks)

b) Misdemeanours (6 marks)

c) Infractions (6 marks)

With the use two (2) of examples, discuss these types of crime

[Total: 20 marks]

QUESTION 3

a) With use of one (1) example, differentiate between Authorization and Accounting features of security. (6 marks)

b) According to research, criminals pursue their self-interests, maximising pleasure and reducing pain, such as material gain, personal safety, and social reputation, and make enemies without caring if they harm others in the process. Do you support or dispute this statement, state reasons for your opinion? (6 marks)

c) Explain any four (4) threats to a fraud detection system. (8 marks)

[Total: 20 marks]

QUESTION 4

Cyber security analysts usually employ more than one of these techniques to help ensure an accurate and comprehensive investigation. These are the specific methods analysts use for collecting data about requirements. These include:

i) Interview, (4 marks)

ii) Questionnaire, (4 marks)

iii) Record inspections (on-site), (4 marks)

iv) Research, (4 marks)

v) Sampling. (4 marks)

Discuss these methods, giving one (1) example in each case.

[Total: 20 marks]

QUESTION 5

a) Data Analysis is the process of systematically applying statistical and/or logical techniques to describe and illustrate, condense and recap, and evaluate data. There are two (2) common types of Data analysis. Using one (1) example, discuss these methods. (6 marks)

b) Describe the following functions used in data analysis

i) Pivot tables (2 marks)

ii) Vlookup (2 marks)

iii) Sorting functions (2 marks)

iv) Sum functions (2 marks)

v) If function (2 marks)

c) According to research, poverty among communities increases the likelihood of criminal behavior such as fraud in business organisations. Discuss this statement. (4 marks)

[Total: 20 marks]

QUESTION 6

a) As an Information Technology investigator, explain how you would go about to perform the following activities:

i) Capture live data (4 marks)

ii) Recover deleted data (4 marks)

iii) Eradicate malware (2 marks)

b) Explain any two (2) reasons why investigators are advised not to turn off routers and other devices during an investigation process. (4 marks)

c) Discuss the process of securing evidence and reporting an incident to law enforcement agencies. (6 marks)

[Total: 20 marks]

QUESTION 7

a) Cyber Crime investigation process typically involves the following stages:

i) Identifying the cyber-crime (2 marks)

ii) Gathering the evidence (3 marks)

iii) Building a chain of custody (3 marks)

iv) Analyzing the evidence (2 marks)

v) Presenting the evidence (2 marks)

vi) Testifying (2 marks)

vii) Prosecution (2 marks)

Describe these stages

b) Discuss the process of gathering evidence on computers hidden partitions. (4 marks)

[Total: 20 marks]

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

BACHELOR OF CYBER SECURITY

CS 340: Cybercrime Investigation and Forensic II

SESSIONAL EXAMINATION

DATE: **TIME: 3 hours**

INSTRUCTIONS

1. Write your Student Identification Number on the Answer Booklet provided
2. This paper has only 2 sections, Section A and Section B. [60 marks]
3. Section A contains open ended questions
4. Section B answer any 3 questions
5. Please write as clearly as possible as illegible handwriting cannot be marked.
6. Number the answers to the questions clearly before answering

---

Section A (Answer all Questions) [4 marks each question]

1. Which of the following is NOT a primary component of digital forensics ontology?
   a) Identification

   b) Preservation

   c) Exfiltration

   d) Analysis

2. What is file carving primarily used for in digital forensics?
   a) Malware analysis

   b) Reconstructing deleted or damaged files

   c) Encrypting files

   d) Network forensics

3. In memory forensics, which of the following is crucial for detecting malware?
   a) Static analysis

   b) Dynamic content analysis

   c) Signature-based detection

   d) Multi-media analysis

4. Open-source Intelligence (OSINT) in cybercrime investigations refers to:
   a) Hacking into secure databases

   b) Gathering publicly available information

   c) Decoding encrypted messages

   d) Extracting data from proprietary systems

5. Which technique is commonly used for fraud detection in forensic investigations?
   a) Data mining

   b) Social engineering

   c) File encryption

   d) Network segmentation

SECTION B (Answer any 3 Questions) [40 marks]

QUESTION 1

During an investigation, you are given a **hard drive** suspected to contain malware. Explain the processes involved in conducting **malware forensics**. Discuss how both static and dynamic analysis can be used to uncover the behavior of the malicious code. **[13.3 marks]**

QUESTION 2

Scenario:

You are investigating a case where a suspect has attempted to delete files from their hard drive. However, you believe the files can be recovered using file carving techniques with a hex editor. The deleted file is a JPEG image that is partially corrupted but still contains identifiable header and footer information.

Task:

Describe the steps you would take to **recover** the deleted JPEG file using a **hex editor**. In your answer, include:

- The signature or markers that identify the start and end of a JPEG file.
- How you would locate these markers within a hex editor.
- The process of extracting the relevant hex data and saving it as a new file. **(7 Marks)**

I. Explain why file carving with a hex editor is useful in digital forensics, particularly when dealing with fragmented or partially corrupted files. **(3.15 Marks)**

II. Discuss any potential **limitations** or challenges of using file carving in this scenario, and how you might overcome them. **(3.15 Marks)**

[13.3 marks]

QUESTION 3

Scenario:

A hard drive has been formatted, and all visible files have been deleted. However, you suspect that important digital evidence still exists on the drive in the form of lost or deleted files. As a forensic investigator, you are tasked with recovering these files using Foremost, an open-source data recovery tool.

Task:

Explain the steps you would follow to perform file recovery using Foremost. In your answer, include:

- How to specify the types of files you are looking to recover (e.g., JPEG, PDF, etc.).
- The command you would use to recover the files from a disk image.
- How the results of the recovery are structured and where the recovered files are stored.

(7 Marks)

Discuss how Foremost is able to recover deleted files from a formatted disk. Explain the importance of file headers and footers in this process. (3.15 Marks)

Identify two possible challenges or limitations when using Foremost for data recovery, and suggest ways to address these challenges. (3.15 Marks)

[13.3 marks]

QUESTION 4

You are tasked with investigating a case of identity theft involving unauthorized access to a company's internal network. Outline the steps you would take to conduct a thorough digital forensic investigation. Include the following in your answer:

- Collection of evidence
- Tools used for analysis
- Steps to preserve the integrity of the evidence

[13.3 marks]

QUESTION 5

Scenario:

During a cybercrime investigation, you suspect that the suspect has used steganography to hide malicious data within an innocent-looking image file. Your task is to analyze the image and uncover any hidden information.

Task:

Kapasa Makasa University

Cybersecurity, Year III, 2024

System Vulnerability Assessment

Cys 330

End of Academic year leaving Examinations

Date: 14/10/2024, 09-12 HOURS **Duration: 3 Hours**

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Seven (7) questions** in this paper. Attempt only **five (5). Question One** is compulsory and choose **any four (4)** from the remaining **seven (7).** Indicate on the Answer sheet your choice from the optional questions.
3. Write your Answers on the answer Sheet provided.

Information to candidates

No Foreign material will be allowed in this examination.

The number of marks is shown in brackets **[ ]** at the end of each question or part question.

Clear handwriting and neat work is encouraged.

The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

Question One [20 Marks] Compulsory

1. Define the following vulnerability assessment terms:
   (a) Typosquatting **[1]**
   (b) Zero-day vulnerabilities **[1]**
   (c) Window of vulnerability **[1]**
   (d) Cybersquatting **[1]**
2. Mention **three (3)** characteristics of a zero-day vulnerability **[3]**
3. As an IT Cybersecurity, you have scanned the system for the organisation you work for. The screenshot below shows the results of the scan.
   (a) Write a Technical Report based on the real time scan on the organisation system. Below, is the guide that could be useful for your answer.
   (i) Title **[1]**
   (ii) Introduction **[1]**
   (iii) Methodology **[2]**
   (iv) Findings **[3]**
   (v) Hypothesis **[2]**
   (vi) Recommendations **[3]**
   (vii) Conclusion **[1]**

Note that using this Screenshot for a real time scanning is optional

---

Optional Questions
Instructions

1. **Choose any other four (4) questions from the six (6) questions below. Note that all questions have the same mark allocations [20 Marks].**
2. **Indicate the choice of your answer on the Answer Booklet provided.**

Question Two [20 Marks]

1. Compare passive and active vulnerability analysis in terms of the following;
   (a) Scalability **[1]**
   (b) Accuracy **[1]**

(c) Effectiveness [1]
(d) Deployment [1]
(e) Resource use [1]
(f) Security vulnerabilities [1]

2. (a) List and explain **two (2)** advantages of Active vulnerability analysis [2]
   (b) List and explain **two (2)** disadvantages of Active vulnerability analysis [2]
   (c) Give and explain **two (2)** advantages of Passive vulnerability analysis [2]
   (d) List and explain **two (2)** disadvantages of Passive vulnerability analysis [2]
3. Compare Internal and External scanners in terms of the following:
   (a) Objectives [1]
   (b) Proactive and reactive [2]
   (c) Scope [1]
   (d) Use cases [1]
   (e) Location [1]

Question Three [20 Marks]

1. Demonstrate the environment in which the following vulnerability assessment technologies below are used;
   (a) Monolithic architecture [2]
   (b) Agent based architecture [2]
   (c) Cloud based architecture [2]
   (d) Multi – source integration [2]
   (e) Agentless based architecture [2]
2. Differentiate between Agent and Agentless architecture [2]
3. Explain possible challenges you are likely to face with an Agent based architecture in terms of false positives, management complexity, scalability concerns and thread vector. [4]
4. Write short notes on monolithic architecture with focus on complexity and rigidity, updating, attack surface and flexibility. [4]

Question Four [20 Marks]

1. Explain briefly in short note form, on hardware vulnerability [2]
2. Write short notes on the following focusing on the explaining what it is and also, the impact and mitigation
   (a) susceptibility to humidity and dusk [3]
   (b) Natural disasters [3]
   (c) Soiling and contamination [3]
   (d) Firmware [3]
3. Discuss software vulnerabilities in terms of;
   (a) Design flaws, impact and mitigation [3]
   (b) Memory safety violations, impact, and mitigation [3]

Question Five [20 Marks]

1. Assess the following with regard to Common Vulnerability Scoring System (CVSS) and also, indicating their colour codes at the end using short notes
   (a) Critical [3]
   (b) High [3]
   (c) Medium [3]
   (d) Low [3]
2. Evaluate the following metric groups below;

(a) Base metrics [1]
  (i) Exploitability metrics [½]
  (ii) Attack vector [½]
  (iii) Attack complexity (AC) [½]
  (iv) User Interaction (UI) [½]
(b) Temporal metrics [1]
  (i) Exploit code maturity [½]
  (ii) Remediation level [½]
(c) Environmental metrics [1]
  (i) Modified base metrics [½]
  (ii) Security requirements [½]

3. Defend the need for Air-gapping in dealing with malware vulnerabilities in an organisation [1]

Question Six [20 Marks]

1. With the aid of a diagram, formulate and explain a Vulnerability Management Lifecycle [[12]
2. Outline **six (6)** bests practices for the act stage in VML [6]
3. Explain the importance of the Tenable Security Centre [2]

Question Seven [20 Marks]

1. Attached, is data to help you answer the questions that follow.

COMPANY DETAILS

- **Company name:** Kapasa Makasa University
- **Location:** Chinsali, Muchinga Province
- **Industry:** Science and Technology
- **Company Size:** 950 Employees

TEST DETAILS

- **Test Start Date:** 1st October 2024
- **Test Duration:** 7 days
- **Network Analysed:** Internal Local Area Network (LAN)
- **Functions enabled:** IPS/AV/Web/APP ctrl

CHALLENGES

- **IPS Attacks detected:** 1,1002
- **Malware and Botnet events detected:** 32
- **High Risks applications detected:** 200
- **Application categories:** Network Service /video/Audio/Web/Others
- **Top Web categories:** Facebook and Instagram/ streaming media and downloading / web-based emails.
- **Top 3 web domains:** Mail. Google.com / stream pandora.com / en.wikipedia.org

NETWORK UTILIZATION

- **Top Hosts/Clients by Bandwidth** 192.0.2.0.24/ 102.130.100.0/102.130.100.255 / 102.144.0.0
- **Average throughput:** 28 Mbps
- **Unique Hosts detected:** 503

ADDITIONAL INFORMATION

- **Evasive applications:** 23
- **P2P and filesharing applications:** 10
- **Bandwidth consuming applications:** 32

Based on the information given above, as a Cybersecurity Expert, write a comprehensive Technical Report for Kapasa Makasa University

Helpful information in no particular order

- **Scan results** **[3]**
- **Executive Summary** **[3]**
- **Risk Assessments** **[3]**
- **Recommendations** **[4]**
- **Findings** **[3]**
- **Methodology** **[2]**

2. Highlight the differences between Macro level and Micro – Level **[2]**

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

CYS 331: WIRELESS SECURITY

SESSIONAL EXAMINATION

DATE: 30-Oct-24 TIME: 09.00 - 12.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Two (2) Sections** in this paper. **Section A is Compulsory and has two (2) questions. Answer any three (3) questions from section B.**
3. Indicate on the Answer sheet your choice from the optional questions.
4. Write your Answers on the answer Sheet provided.
5. No Foreign material will be allowed in this examination.
6. The number of marks is shown in brackets **[ ]** at the end of each question or part question.
7. Clear handwriting and neat work is encouraged.
8. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

SECTION A: ANSWER BOTH QUESTIONS

QUESTION 1

When designing a wireless network, it's important to follow standard security practices so that the network cannot be compromised by hackers.

a) Explain in detail how you would ensure that only authorized users access the wireless network. **[4 Marks]**
b) Explain in detail how you would ensure that only legitimate access points enable network connectivity to the wireless users. **[4 Marks]**
c) Explain in detail how you would ensure only legitimate devices can connect using the wireless network. **[4 Marks]**
d) List and explain four (4) ways in which wireless clients can be assigned IP addresses. Hint: state how DHCP can be implemented. **[8 Marks]**

Total Marks: 20

QUESTION 2

a) Briefly explain why the BYOD policy is important to protect wireless networks. **[2 Marks]**
b) Briefly explain how you can implement AAA on a wireless network. **[6 Marks]**
c) List and explain three (3) mobile data standards used a cellular network **[6 Marks]**
d) State two differences between frequency-hopping and direct-sequence spread spectrum. **[6 Marks]**

Total Marks: 20

SECTION B: CHOOSE ANY THREE (3) QUESTIONS

QUESTION 3

IP security in wireless networks is crucial to protect data integrity, confidentiality, and availability.

a) Mention and explain five (5) protocols implemented by IP security. **[10 Marks]**
b) To achieve successful association, a wireless client and an AP must agree on specific parameters. Mention and explain the use of each parameter. **[10 Marks]**

Total Marks: 20

QUESTION 4

Ensuring your Wi-Fi network is secure is crucial to protect your data and privacy.

a) Mention and explain five (5) measures that should be implemented in order to secure the wireless network. **[10 Marks]**
b) Going by the customer's requirements, users on the wireless network should not have access to the server segment. However, they can only communicate with users on the printing segment and can also access the internet. Explain in detail how your design will implement these requirements. Hint: your network should use a 1941 router. **[10 Marks]**

Total Marks: 20

QUESTION 5

A WLAN operates in the same manner as a wired LAN except that data is transported through a wireless medium—usually radio waves—rather than cables.

a) Mention and explain four (4) vulnerabilities found in wireless networks. **[8 Marks]**

b) Mention four (4) types of wireless network security protocols. In addition, using a table state their differences in terms of their level of security and authentication. **[12 Marks]**

Total Marks: 20

QUESTION 6

a) Briefly explain the use of SSL/TLS in wireless networks. **[4 Marks]**

b) Mention and explain five (5) Bluetooth common security risks. **[10 Marks]**

c) List and explain three (3) wireless topology modes. **[6 Marks]**

Total Marks: 20

QUESTION 7

a) Explain in detail how you can configure a home wireless router. State what security measures you will take to make it secure. **[8 Marks]**

b) Explain in detail the methods used by wireless clients to connect to the access point. You should clearly show how data is exchanged between the client and access point in both instances. **[8 Marks]**

c) What is the difference between a piconet and scatternet in Bluetooth networks. **[4 Marks]**

Total Marks: 20

END OF PAPER

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

CYS 335

ACCESS CONTROL AND INTRUSION DETECTION

SESSIONAL EXAMINATION

DATE: 04-Nov-2024 TIME: 14.00 - 14.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Six (6) questions** in this paper. Attempt any **five (5).** Indicate on the Answer sheet your choice from the optional questions.
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets **[ ]** at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION 1

a) At times because of lack of expertise in certain areas, Organizations tend to contract some works from other organizations. You are a senior Cyber Security Specialist working closely with the contractor. How should temporary access be managed for a contractor working on a short-term project?

[3 Marks]

b) "Cyber Attacks are inevitable and we have to live with them". Therefore what role can honeypots play in enhancing an IDS's effectiveness? [3 Marks]

c) Explain how integrating access control with IDS contributes to a multi-layered defense strategy.

[3 Marks]

d) It has been argued that warning increase the sense of fear in potential criminals. In what ways can publicizing the presence of security cameras deter unauthorized access to sensitive areas?

[4 Marks]

e) What role does regular security training play in deterring employees from engaging in unsafe practices? [4 Marks]

f) What measures would you put in place to prevent data breaches in a cloud computing environment? [3 Marks]

QUESTION 2

a) Tokens are said to have better security than passwords. Explain the mechanism of an asynchronous based token authentication [4 Marks]
b) How would you restore customer confidence in your organization following a publicized security incident? [2 Marks Each]
c) To easy implementation of access control, a number of concepts or abstract ideas have been developed. Describe the following implementation of an Access Control Matrix:
    a. Access Control List [3 Marks]
    b. Capability List [3 Marks]
d) There several password attacks that an attacker might use. You are required to identify Four(4) of them and suggest mitigation measure respectively. [8 Marks]

QUESTION 3

a) What steps should be taken to secure remote access to the corporate network? [5 Marks]

b) How would you use audit logs to support non-repudiation in case of a dispute? [5 Marks]

c) What steps should be taken if an IDS detects an unauthorized remote access attempt that bypassed the access control system? [5 Marks]

d) Explain how integrating access control with IDS contributes to a multi-layered defense strategy.

[5 Marks]

"Success Comes in Cans and Failure in Can't s"

If access control logs indicate possible compromised credentials and an IDS confirms suspicious activity from the related account, how should the situation be handled? [5 Marks]

QUESTION 4

Technical control is at the very core of access control. Technical controls called logical controls are the software tools used to restrict subject's access to objects.

Identify and explain four (4) of the control components [5 Marks Each]

QUESTION 5

At a company named "NSHALIKO" the administration had a notion that every aspect of Cyber security is for the ICT Department of the organization and that administration had nothing to do with it. It was discovered that despite the ICT Department doing it's level best, there where still some security challenges here and there. You are now invited to present to the company missing gaps in cyber security to highlight to the management that it has a significant role to play in access control contrary to some ideas that this role is purely technical. Your presentation includes the following suggestions. Explain how each of them is important and may be used:

i) Security Awareness Training [4 Marks]

ii) Supervisory structure [4 Marks]

iii) Testing [4 Marks]

iv) Personel Controls [4 Marks]

v) Policies and procedures [4 Marks]

QUESTION 6

a) What role does regular security training play in deterring employees from engaging in unsafe practices? [3 Marks]

b) Auditing is an important part of system security. Elaborate briefly on what auditing constitutes. [3 Marks]

c) Mention and briefly explain 5 of the best practices of authentication and Access control [2 Marks Each]

d) How can a honeypot system be used to deflect attacks from critical systems? [4 Marks]

CYBER SECURITY 2025 YEAR 1 TO 4

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING
DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY
BACHELOR OF SCIENCE IN CYBER SECURITY

COURSE CODE CYS 100 - NETWORK DESIGN AND ADMINISTRATION

FINAL EXAMINATION

Date: **Duration:** **3 Hours** **Total Marks: 100**

INSTRUCTIONS

1. Write your **Student Identification Number** on the **Answer Booklet** provided
2. Do not turn this page until you are told to do so
3. This Question paper contains **7** Questions; attempt 5 questions
4. Questions **1** and **2** are compulsory
5. **Calculators** are **NOT** allowed in the **Examination Room**
6. **No** foreign material is allowed in the **Examination Room** except as stated
7. **Start** each answer on a new page
8. **All** questions carry equal marks

[Question 1]

A. Discuss the evolution of computer networking from early resource sharing to modern Internet infrastructure. How has the concept of locality of reference influenced LAN design? **[6 Marks]**

B. Compare and contrast the following transmission media in terms of bandwidth, distance limitations, and susceptibility to interference: **[9 Marks]**

i. Unshielded Twisted Pair (UTP) vs. Shielded Twisted Pair (STP)

ii. Single-mode vs. Multi-mode fiber optic cables

iii. Geostationary vs. Low Earth Orbit (LEO) satellite communication

C. Explain how noise affects digital communication systems. Describe three techniques used to minimise noise impact in modern network implementations. **[5 Marks]**

[Question 2]

A. Given the network address 10.0.0.0/8, an organisation needs to create subnets for 500 departments, with each department requiring at least 100 host addresses. **[8 Marks]**

i. Determine the appropriate subnet mask in CIDR notation and dotted decimal format.

ii. Calculate the total number of subnets that can be created.

iii. Specify the network and broadcast addresses for the 5th subnet.

B. A company has the IP address range 203.45.78.0/25. **[7 Marks]**

i. Calculate the number of usable host addresses

ii. Identify the subnet mask in binary and dotted decimal notation

iii. Determine if the IP address 203.45.78.140 belongs to this network

C. Explain the advantages of Variable Length Subnet Masking (VLSM) over traditional fixed-length subnetting. Provide a practical scenario where VLSM would be beneficial. **[5 Marks]**

[Question 3]

A. Describe the role of modulation in digital communication. Explain the differences between Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), and Phase Shift Keying (PSK). **[7 Marks]**

B. Analyse the differences between baseband and broadband transmission technologies. Discuss how these technologies are implemented in modern Ethernet and cable TV systems. **[8 Marks]**

C. Explain Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM). How do these techniques optimise bandwidth utilisation? **[5 Marks]**

[Question 4]

A. Describe how packet switching enables efficient network communication. Explain the relationship between packets and statistical multiplexing. **[6 Marks]**

B. Compare the following error detection and correction mechanisms: **[9 Marks]**

i. Single-bit and two-dimensional parity checking

ii. Internet checksum algorithm

iii. Cyclic Redundancy Check (CRC) with polynomial division

C. Explain the concept of frame synchronisation and the need for byte stuffing. Illustrate with an example how the Data Link Escape (DLE) character is used in byte stuffing. **[5 Marks]**

[Question 5]

A. Differentiate between point-to-point and multi-access communication channels in LAN environments. **[4 Marks]**

B. Evaluate the three primary LAN topologies (bus, ring, and star). For each topology, discuss: **[12 Marks]**

i. Physical implementation and logical operation

ii. Fault tolerance characteristics

iii. Scalability considerations

iv. Modern applications and variations

C. Describe Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and explain why it is not suitable for modern full-duplex switched networks. **[4 Marks]**

[Question 6]

A. Explain the structure and significance of MAC addresses in LAN communication. Describe how broadcast, multicast, and unicast addressing work at the data link layer. **[6 Marks]**

B. Analyse the evolution of Ethernet wiring standards: **[9 Marks]**

i. 10BASE5 (Thick Ethernet) and its limitations

ii. 10BASE2 (Thin Ethernet) improvements and drawbacks

iii. 10BASE-T and modern twisted-pair implementations (100BASE-TX, 1000BASE-T)

C. Discuss the functionality of Network Interface Cards (NICs) in modern networking. What considerations are important when selecting NICs for high-performance network applications? **[5 Marks]**

[Question 7]

A. Explain the distance limitations inherent in LAN technologies and how fiber optic extenders and repeaters address these constraints. What are the differences between repeaters and amplifiers? **[6 Marks]**

B. Compare the operational characteristics and applications of the following network devices: **[9 Marks]**

i. Layer 2 switches and their frame forwarding mechanisms

ii. Network bridges and spanning tree protocol

iii. Layer 3 routers and routing table operations

C. Contrast the following network architectures and provide contemporary examples: **[5 Marks]**

i. Local Area Networks (LANs) in enterprise environments

ii. Wide Area Networks (WANs), including SD-WAN implementations

iii. Metropolitan Area Networks (MANs) and their role in smart cities

The End

All the best!

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM

Course Title: Cryptography

Course Code: CYS 110

Date: 30TH JULY 2025

Duration: 3HRS

Total Marks: 100

General Instructions to Candidates:

1. Answer questions 1 and 2 and any other 3 three questions.
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

[QUESTION 1]

Namesake Sakala is the team leader for the infant brigade in Ukraine defending the country against the Russian Invasion. He wants to transmit the clear message to his soldiers **''we have been discovered run for your lives and report to the base''** using vigenere cipher with the key **''FOUND''**.

A. Encrypt the message to be sent. [2 Marks]
B. Assuming you did not know the key length, use Kasiskie and/or Friedman tests to get the key length. [3 Marks]
C. Find the numbers for key you have found in B above. [3 Marks]
D. Use the appropriate Vigenere cipher formulas of your choice to decrypt the encrypted message in A. [12 Marks]

[QUESTION 2]

A. As Israel continues to fight Iran. The IDF Commander need to send the message **''Attack from front''** to their Soldiers using AES with the key of **''Fighting is over''**. Use the Hex ASCII table provided to convert the message and key to hexadecimal values. [5 Marks]
B. Using AES algorithm, encode the hexadecimal message in A above using Rinjndael Algorithm with the round key in B. The S-Box and Predefined matrix are given on the final page. [15 Marks]

[QUESTION 3]

A. Alice and Bob are running a financial business located in Kitwe and Lusaka respectively. They have decided to share the daily financial data via a new symmetric key every day. On a particular day they have picked two prime numbers 13 and 11 as their g and n values and 3 and 5 as random numbers respectively. Use the two values to come up with the symmetric key using Deffie-Hellman Algorithm. [7 Marks]
B. Use mathematical theory to prove why Alice and Bob's key are same in A above. [7 Marks]
C. Assuming Trudy intercepted the communication between Alice and Bod when they were exchanging values for g and n in A and decided to come up with his random numbers 4 and 6. Mathematically show how Trudy would succeed to launch a man in the middle attack. [8 Marks]

[QUESTION 4].

A. Mention and explain any two types of ciphers under the Stream and Block ciphers.

[2 Marks]

B. If P*i* is the *i*th digit of the plain text, C*i* is the *i*th digit of the cipher text and K*i* is the *i*th digit of the key. Write down the encryption and decryption equations assuming that we are using a modified Polyalphabetic vigenere cipher that uses character of hexadecimal digits. [7 Marks]

C. If the clear text is A 5 0 8 C 2 A 7 and the Key is 1 7 C E 1 6 F 4.What is the Cipher text? [7 Marks]

D. Polyalphabetic ciphers such as the above Vigenere cipher is stronger against letter frequency analysis when compared to monoalphabetic ciphers like Caesar ciphers. Explain why it is so. [4 Marks]

[QUESTION 5].

A. Admin block at KMU has just connected a network consisting of N computers, each of these computers is running a network application for file sharing. If session keys are needed for the secure communication, come up with a formula for finding the total number of session keys in this network. [2 Marks]

B. Use the Formula above to find the total number of session keys needed in a network with 10 hosts of computers running two applications. [4 Marks]

C. You have received a message YPESEEDTYICOEACRTLRATOIMOURBPHSTYVYRAHESNUGSPUCSC together with the key **Frame it**. Decode the message using an appropriate stream cipher. [8 Marks]

D. With the help of an appropriate diagram, explain how encryption using a DES block cipher is achieved. [6 Marks]

[QUESTION 6].

A. Differentiate between chosen plain text attack and known plain text attack. [2 Marks]

B. You are required to send the message **HELP ME PLEASE** to your friend using a block cipher that is using modulo 27 because the English alphabet has been extended to include a space as a character. Assuming the first letter starts from 1,

encrypt the message above if the encryption key K_C = || and the decryption key K_P= || [7 Marks]

C. Use the Decryption Key provided above to decrypt the cipher text you have gotten in A. [7 Marks]

D. Using the same modulo 27 above, if the Encryption Key is given as K_C= || find the decryption key K_P that will be used to decrypt the cipher text. [4 Marks]

[QUESTION 7].

A. Explain why someone might opt to use encrypt a message with hush function like MD5 father than public key like RSA. [2 Marks]

B. You have received a message **UTLAIKNP** encrypted with the key (33, 7). Find the private keys that should be used to decrypt the message and work out the clear text. [7 Marks]

C. Clearly explain how public key cryptography is an excellent candidate for providing authentication and message integrity. Use the aid of suitable diagrams in your explanations. [7 Marks]

D. With an appropriate example explain how a one-time password can be used to prevent a replay attack. [4 Marks]

Helpful Information

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

CYS 111: SECURE SOFTWARE ENGINEERING

2025 SESSIONAL EXAMINATION

DATE: 5th November 2025 **TIME: 3 hours** **TOTAL MARKS: 60 MARKS**

INSTRUCTIONS

1. Write your Student Identification Number on the Answer Booklet provided
2. **Answer all Questions in Section A.**
3. **Answer any THREE (3) Questions in Section B.**
4. Please write as clearly as possible as illegible handwriting cannot be marked.
5. Number the answers to the questions clearly before answering

SECTION A: Each Question Carries 4 Marks

1: What is software engineering?

2: What is a software process or Software Development Life Cycle (SDLC)?

3: What are some SDLC models available?

4: What is the difference between verification and validation?

5: Difference between functional and non-functional requirements.

SECTION B: Each Question Carries 20 Marks

1. Describe the importance of software Engineering? What should be steps taken under the process of developing a software system. **[13.3 Marks]**

2. Giving reasons for your answer based on the type of system being developed, suggest the most appropriate generic software process model that might be used as a basis for managing the development of the following systems:

a. A system to control anti-lock braking in a car
b. A virtual reality system to support software maintenance
c. A university accounting system that replaces an existing system
d. An interactive travel planning system that helps users plan journeys with the lowest environmental impact **[13.3 Marks]**

3. Explain the following;

a. Why the rapid delivery and deployment of new systems is often more important to businesses than the detailed functionality of these systems.
b. Why programs that are developed using evolutionary or agile development are likely to be difficult to maintain. **[13.3 Marks]**

4. Describe the following;

a. The differences between 1) Requirements Elicitation, 2) Requirements Definition, and 3) Requirements Specification.
b. Four types of non-functional requirements that may be placed on a system. Give examples of each of these types of requirement. **[13.3 Marks]**

5. Briefly explain the following;

a. What is Agile?
b. What are the benefits of Agile Software development?
c. What is the Agile Manifesto (state its core values)? **[13.3 Marks]**

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAMINATION

Course Title: Cyber Threats Intelligence
Course Code: CYS 210
Date: OCTOBER 2025
Duration: 3HRS
Total Marks: 100

General Instructions to Candidates:

1. Strictly follow instructions in each section please.
2. Use examples, diagrams, and real-life case studies where appropriate.
3. Ensure your answers are well-structured and legible.
4. No unauthorized materials are allowed
5. No electronic devices are allowed unless specified.
6. Start each answer on a new page.
7. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

Section A MCQ (10 Marks)

Answer all questions in this Section.

Choose the best option by writing the letter of your choice on the answer sheet.

1. When an organization collects and analyzes information about cyber threats to predict future attacks, what is this process called?
   (A) Cyber Threat Intelligence.
   (B) Software Development.
   (C) Data Archiving.
   (D) Network Maintenance.
2. Which common cyber threat tries to trick users into giving away personal information through fake emails or websites?
   (A) Phishing.
   (B) Antivirus.
   (C) Firewall.
   (D) Backup.
3. Which tool is generally used to protect a computer network from unauthorized access?
   (A) Calculator.
   (B) Web Browser.
   (C) Word Processor.
   (D) Firewall.
4. What is the primary purpose of cyber threat intelligence for organizations?
   (A) To monitor how fast the internet connection is.
   (B) To help organizations understand and prepare for potential digital attacks.
   (C) To create new computer games for employees.
   (D) To automatically fix all computer problems instantly.
5. What action is the key part of responding to a detected cyber-attack?
   (A) Ignoring the attack to see if it stops on its own.
   (B) Isolating affected computer systems to prevent further spread.
   (C) Sharing personal login details with the attackers.
   (D) Downloading more software from unknown sources.

6. What does a strong password typically include to make it secure?
   (A) Just a common word or name.
   (B) Only lowercase letters and numbers.
   (C) Only numbers in sequential order.
   (D) A combination of uppercase letters, lowercase letters, numbers, and symbols.
7. What is a cyber threat in the context of digital security?
   (A) Any potential danger that can harm digital systems or data.
   (B) A program that helps computers run faster.
   (C) A type of online game played by many people.
   (D) A method for storing files safely on a cloud.
8. What is an Indicator of Compromise (IoC)?
   (A) firewall configuration file
   (B) Evidence that a system has been breached
   (C) A software update
   (D) An antivirus signature
9. Which of the following best describes "tactical threat intelligence"?
   (A) High-level information for executives and board members
   (B) Real-time data used for intrusion detection
   (C) Information about adversaries' motives and capabilities
   (D) Logs collected from a security information and event management (SIEM) system
10. Which framework is commonly used in Cyber Threat Intelligence to describe attacker behavior?
   (A) ISO/IEC 27001
   (B) MITRE ATT&CK
   (C) NIST 800-53
   (D) GDPR

Section B– Descriptive Questions (6 × 10 = 60 Marks)

Answer SIX questions only.

1. Define Cyber Threat Intelligence (CTI). Explain the types of threat intelligence (Strategic, Tactical, Operational, and Technical) with real-world examples. **(10 Marks)**

2. Describe the Cyber Threat Intelligence lifecycle. Explain each phase with examples and discuss how this lifecycle supports proactive defense mechanisms. **(10 Marks)**
3. What are Indicators of Compromise (IOCs)? Provide examples of different types of IOCs and explain how they are used in identifying cyber threats. **(10 Marks)**
4. Compare and contrast the following intelligence sources:
   (a) Open-Source Intelligence (OSINT)
   (b) Human Intelligence (HUMINT)
   (c) Signals Intelligence (SIGINT)
   (d) Technical Intelligence (TECHINT)
   Discuss their relevance in CTI. **(10 Marks)**
5. What is the role of Threat Intelligence Platforms (TIPs) in security operations? Discuss at least two commercial and one open-source TIP, highlighting their features and practical use. **(10 Marks)**
6. Explain how MITRE ATT&CK framework is used in threat intelligence analysis. Choose one threat actor group and analyze their tactics and techniques using this framework. **(10 Marks)**
7. A small organization is experiencing frequent phishing attacks. Describe how Cyber Threat Intelligence can be used to analyze, prevent, and respond to such attacks. Include practical tools, analysis methods, and reporting techniques. **(10 Marks)**

Section C – Long Essay Questions (2 × 15 = 30 Marks)

Answer TWO questions only.

8. You have been appointed as a CTI Analyst for a critical infrastructure company. Develop a CTI Strategy Plan covering the following:
   i. Identification of internal and external data sources
   ii. Intelligence collection and analysis process
   iii. Reporting and dissemination strategy
   iv. Legal, ethical, and privacy considerations
   v. Support your answer with a real-world case or scenario.
9. Conduct a practical threat actor profiling exercise based on an APT group (e.g., APT29, Lazarus Group, or Fancy Bear). Your analysis should include:
   i. Historical background and attribution

ii. Attack lifecycle

iii. Tools, Tactics, and Procedures (TTPs)

iv. Targeted sectors and geographies

v. Defense and mitigation strategies

vi. Use threat intelligence frameworks and tools where applicable.

10. Discuss the integration of threat intelligence with SIEM systems in a Security Operations Center (SOC). Your answer should cover:

i. Real-time threat detection

ii. Correlation rules and enrichment

iii. Case study of SIEM + CTI integration

iv. Challenges and best practices

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES

CSY211 – SOCIAL NETWORK ANALYSIS
2025 SESSIONAL EXAMINATIONS

Date: 29th October 2025

Instructions :

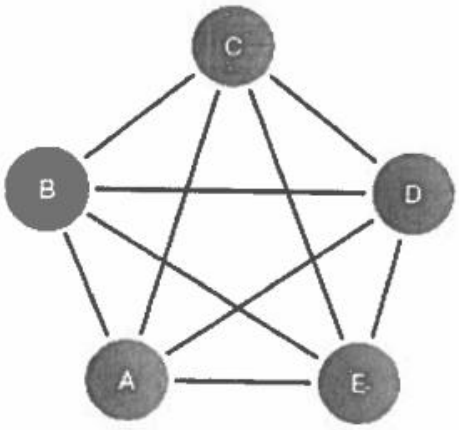
1. Time allowed is **three (3) hours**
2. There are **Seven (7) Questions** in this paper.
3. You are required to answer any **Five (5)** questions.
4. Total Marks: **100**.

Question 3 [20 Marks]

Graph Theory is a field of discrete mathematics that deals with the study of graphs, which are abstract representations of a set of objects where some pairs of the objects are connected by links.

a. Define the following terms in graph theory
   i. Tie Set **[2 Marks]**
   ii. Link **[2 Marks]**
   iii. Terminal Node **[2 Marks]**

b. For the given complete graph below



   i. Find the number of Trees and Co-Trees **[4 Marks]**
   ii. Plot one Tree, Co-Tree **[2 Marks]**
   iii. Show the twig and links **[4 Marks]**
   iv. Show the adjacency Matrix for the given graph **[4 Marks]**

Question 4 [20 Marks]

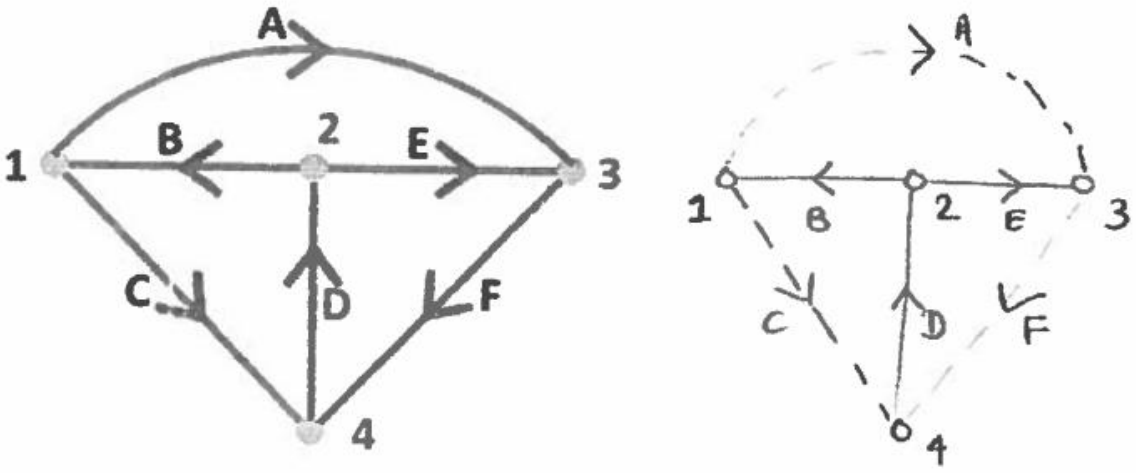
a. Define the following terms in graph theory
   i. Twig **[2 Marks]**
   ii. Cut Set **[2 Marks]**

vi. Draw the Cut Set Graph and direction of Links and Twigs ,on how the connection **[4 Marks]**

b. Give two applications of Cuts Sets in Cyber Security? **[2 Marks]**

Question 6 [20 Marks]

a. For the given Graph below and its corresponding Tie Set Graph with a tree (BED) and Co-Graph (CAF)



Find the

i. Tie Set Matrix **[4 Marks]**
ii. Number of Links **[2 Marks]**
iii. Number of Twigs **[2 Marks]**
iv. Number of Loops **[2 Marks]**

b. Give four importance of Tie Sets in Cyber Security? **[4 Marks]**

c. List and describe three software tools ,techniques used in social network analysis **[6 Marks]**

Question 7 [20 Marks]

a. Network Data can be represented and stored in various formats depending on the tools being used and the structure of the data. These formats define how nodes (vertices)and edges (links)are recorded. Describe the formats below and give an example for each.

i. JSON-based Formats **[2 Marks]**
ii. PajekFormat **[2 Marks]**
iii. GraphML(Graph Markup Language) **[2 Marks]**
iv. Adjacency Matrix **[2 Marks]**

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM

Course Title: Penetration Testing

Course Code: CYS 212

Date: 12TH November 2025

Duration: 3HRS

Total Marks: 100

General Instructions to Candidates:

1. Answer **All** questions in **Section A** and any other **(4) four** questions in **Section B.**
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

SECTION A: 20 MARKS

Answer all questions from this section by writing only the letter that corresponds to the best answer from the given options.

1. Which of the following best describes a Rule of Engagement (RoE) in a penetration test?
   A. A signed contract that lists software licenses to be used.
   B. A technical report template for vulnerability findings.
   C. A document that defines scope, timing, authorisation, and allowed actions for the test.
   D. A backup plan for restoring production systems.

2. Passive reconnaissance differs from active reconnaissance primarily because:
   A. Passive uses only scanners like nmap; active uses OSINT.
   B. Passive does not interact directly with the target's systems; active does.
   C. Passive always requires authentication; active does not.
   D. Passive is always illegal while active is legal.

3. Which tool is most commonly used for discovering WordPress plugins and themes remotely?
   A. Nessus
   B. WPScan
   C. Aircrack-ng
   D. Metasploit

4. Enumeration is distinct from scanning because enumeration:
   A. Is only concerned with wireless networks.
   B. Identifies and interacts with services to gather usernames, shares, and detailed information.
   C. Exclusively uses passive DNS lookups.
   D. Only finds open ports without service details.

5. Which port is typically associated with SMB and often targeted for Windows file-share exploits?
   A. 22
   B. 80
   C. 445
   D. 3389

6. Which of these tools is primarily used for capturing WPA/WPA2 handshakes on Wi-Fi networks?
   A. Airodump-ng
   B. theHarvester
   C. dnsenum
   D. sqlmap

7. A false positive in a vulnerability scan means:
   A. A vuln reported that does not actually exist.
   B. A vulnerability that has been publicly disclosed.
   C. A confirmed exploit in the wild.
   D. A vulnerability that affects only deprecated protocols.

8. The Social Engineering Toolkit (SET) is best used for:
   A. Password cracking using GPU acceleration.
   B. Crafting phishing pages and social engineering simulations.
   C. Discovering subdomains via DNS zone transfers.
   D. Brute-forcing SSH credentials.

9. Which OpenVAS/Nessus output would most likely indicate an authenticated scan was performed?
   A. A list of only open TCP ports.
   B. High-confidence findings that include registry or configuration details.
   C. A handshake capture file.
   D. A list of public DNS records.

10. In a Red Team engagement, a "pivot" refers to:
    A. Using powerline adapters to extend Wi-Fi.
    B. Moving from a compromised host to other internal systems.
    C. Reporting vulnerabilities to management.
    D. Restoring systems after testing.

11. The Metasploit Meterpreter payload is primarily used for:
    A. Passive DNS enumeration.
    B. Interactive post-exploitation control of a compromised host.
    C. Generating SSL certificates.
    D. Performing brute-force attacks on SSH.

12. Dragonblood vulnerabilities relate to which wireless standard?
    A. WPA2
    B. WPA3
    C. WEP
    D. 802.1X EAP-TLS

13. Which method is the best for validating a suspected SQL injection found by automated scanning?
    A. Trust the scanner only and list the finding.
    B. Manually reproduce the injection with safe, controlled payloads and a proof-of-concept.
    C. Perform a denial-of-service to confirm.
    D. Immediately exploit and exfiltrate data.

14. SS7 protocol vulnerabilities are primarily a threat to:
    A. Web servers' SSL certificates.
    B. Telecom signaling and SMS/voice interception.
    C. IoT over LoRaWAN.
    D. Wi-Fi handshake security.

15. In cloud pentesting, an IAM misconfiguration can lead to:
    A. Weak wireless handshake capture.
    B. Excessive privilege escalation or data exposure.
    C. Faster brute-force password cracking.
    D. DNS zone transfer denial.

16. Which of the following best describes a "supply chain attack"?
    A. An attacker intercepts supply truck logistics physically.
    B. Compromising a third-party component or API to affect the primary target.
    C. Tampering with Modbus traffic in SCADA networks.
    D. Performing phishing only against supply chain staff.

17. Which of these tools is commonly used for subdomain enumeration?
    A. Aircrack-ng
    B. dnsenum
    C. John the Ripper
    D. Airodump-ng

18. What is the primary ethical concern when simulating ransomware during a test?
    A. Whether it uses open-source code.
    B. Potential destructive effects on live data and availability.
    C. The length of the test report.
    D. The number of tools used.

19. In a MiTM (Man-in-the-Middle) attack, the attacker typically:
    A. Only scans for open ports without interception.
    B. Intercepts and possibly modifies communications between two parties.
    C. Uses only passive OSINT methods.
    D. Performs only privilege escalation on hosts.

20. A good executive summary in a pentest report should:
    A. Contain raw exploit commands used.
    B. Use technical jargon to impress readers.

C. Summarize key risks, business impact, and prioritized remediation in plain language.

D. Include all screenshots and logs verbatim.

SECTION B: 80 MARKS

Answer any four (4) questions from this section

[QUESTION 1]

As the lead IT administrator at Ndola General Hospital, you have been tasked with assessing the security of the hospital's electronic medical records (EMR) system, which runs on an outdated PHP backend.

a) Construct a penetration testing plan targeting EMR SQL injection vulnerabilities, including tools and expected outcomes. [10 Marks]
b) Analyze the ethical implications of exposing sensitive medical data such as HIV patient records during penetration testing and describe safeguards you would implement. [10 Marks]

[QUESTION 2]

You were contracted as a penetration tester and digital forensics consultant after an incident where a Russian hacker is accused of intercepting communications between Ukraine and the USA. Your assessment captured packet traces, system logs, and Meterpreter artifacts from a compromised host.

a) Explain the steps you would take to collect, preserve, and document digital evidence so it is admissible in court. Include chain-of-custody procedures, hashing, timestamping, and how you would avoid contamination. [10 marks]

b) As the technical expert called to testify, outline how you would present technical findings to a non-technical judge or jury, explain attribution limitations (e.g., spoofing, proxy, false flags), and describe collaboration with international law enforcement given cross-border implications. [10 marks]

[QUESTION 3].

You are engaged as a senior wireless security assessor by the Electoral Commission of Zambia to test the campus Wi-Fi used by election officers and polling station coordinators. The assessment must consider the sensitivity of election-related sessions.

a) Demonstrate how you would capture traffic and perform a Man-in-the-Middle (MITM) attack on a Wi-Fi network using tools such as airodump-ng, aireplay-ng, and ettercap. Include commands, expected artifacts (e.g., captured handshakes, ARP poisoning outputs), and how you would identify authenticated session tokens (cookies, JWTs) in traffic. [12 Marks]
b) Explain the mechanics of session hijacking once a session token is captured, discuss real-world impacts to election integrity, and recommend immediate mitigations and secure configuration changes the Commission should implement. [8 marks]

[QUESTION 4].

As a senior network administrator at the Zambia Air Force, you are tasked with evaluating the security of the military base's Wi-Fi infrastructure to ensure it is resilient against cyber intrusions.

a) Demonstrate how you would use Airodump-ng and Aircrack-ng to capture WPA2 handshake packets and attempt a dictionary attack. Include commands and expected outputs. [12 marks]

b) Critically analyze the ethical and national security implications of performing dictionary attacks versus brute-force methods during penetration testing in a military environment. [8 marks]

[QUESTION 5].

You have been hired as penetration testing intern at Kapasa Makasa University. On your first day of work, your manager asks you to assess their external network using a computer that runs on Kali Linux.

a) Describe how you would carry out passive reconnaissance using tools such as whois, theHarvester, and Google dorking. Provide expected outputs [10 Marks]
b) The target has deployed defense mechanisms against passive OSINT. Explain and demonstrate how you would escalate to active reconnaissance using nmap and discuss the risks of detection. [10 Marks]

[QUESTION 6].

During an assessment of a government web server, you discover open ports 22, 80, and 445.

a) Using Nmap and Netcat, demonstrate how you would enumerate services running on each port. Include commands and sample outputs. [10 Marks]
b) Evaluate how enumeration findings can directly influence the choice of potential exploits and exploitation strategies. [10 Marks]

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM

Course Title: Ethical Hacking

Course Code: CYS 220

Date:

Duration: 3HRS

Total Marks: 40

General Instructions to Candidates:

1. Answer a compulsory question 1 and any other 3 of your choice.
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

[QUESTION 1 Compulsory**]**

For Windows OS especially, it is important to implement a schedule for vulnerability assessments or scanning. Windows is popular and easy to navigate, and it's a favorite with hackers. So, there are some free software available on the market for such tasks. Outline a **detailed** step-by-step procedure on how to crack Windows Admin Login Account using CMD.

[10 Marks]

[QUESTION 2]

1) Define Session Hijacking [2 Marks]
2) Explain Denial of Service [2 Marks]
3) Give at least two countermeasures to Session Hijacking [2 Marks]
4) What's the common goal between a Hacker and a Cracker? [2 Marks]
5) Give reasons to why its easier to Hack Windows OS than Linux OS [2 Marks]

[QUESTION 3]

1) What is Enumeration? [2 Marks]
2) The three basic types of scanning are Port, Network and Vulnerability. State what is involved at each of these stages. [2 Marks]
3) What are the two basic types of Intrusion detection Systems? [2 Marks]
4) Is google.com a search engine or web browser? [2 Marks]
5) What's the difference between Cyber Security and Information Security? [2 Marks]

[QUESTION 4]

1) What is Social Engineering? [2 Marks]
2) Outline the two common types of Social engineering [2 Marks]
3) What is Art of Manipulation? [2 Marks]
4) What is Phishing? [2 Marks]

5) The two common attacks are Insider and Outsider. Give an example of each category?

[2 Marks]

[QUESTION 5]

1) What is Hacking?

[2 Marks]

2) What is Ethical Hacking? [2 Marks]

3) List the three types of Hackers by giving examples in each category [2 Marks]

4) List all the Stages of the Hacking Cycle [2 Marks]

5) What's the difference between Hacking and Cracking? [2 Marks]

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES

BACHELAOR OF SCIENCE IN CYBER SECURITY

DIGITAL FORENSICS AND CYBERCRIME INVESTIGATION

COURSE CODE: CYS 230

FINAL EXAMINATION

DURATION: Three hours (5 MINUTES TO READ THROUGH THE PAPER)

INSTRUCTIONS

1. There are **seven** questions in this paper. Question **One** is **compulsory.** Answer any **four** more questions from Question **Two** to Question **Seven**

2. The examination paper carries a total of **60 marks**. Marks are allocated at the end of each question accordingly.

3. Candidates are permitted to extract the following unmarked statues into the examination room;
   (i) The Cyber Crimes Act Number 4 of 2025
   (ii) Evidence Act and,
   (iii) National Forensics Act No. 2 of 2020

4. use of any other extra materials other than what has been permitted will be deemed malpractice.

5. Make sure to write all the necessary details on the answer sheet provided. Use of a neat and clear handwriting is encouraged.

6. **Candidates must not turn this page until told to do so by the Supervisor of this examination**

Question One [20 Marks]

Read the following and answer the questions that follow;

Japhet, a renound and well-trained Computer expert has been a reliable Cyber security Expert for a well-known Internet Service Provider company in Chinsali town. Part of his duties included such responsibilities as; safeguarding digital assets of the organisation from computer theft and damage, or unauthorised access by developing and implementing security measures, protect clients on a network, analyses and investigate threats and vulnerabilities, design and operate security systems, monitor networks for attacks, respond to incidents, and ensure the organisation's overall cybersecurity posture is strong and up to date. However, the Company has established that Japhet, their reliable IT personnel has been involved in illicit activities such as interfering with the network system, cyber extortion and company espionage, data breaches and linking wire fraud investigations to a close friend in the Accounts department.

(a) You have been approached for legal opinion based on the Cybercrimes Act No. 4 of 2025 and further, punishment administered to anyone who contravenes the sections and or subsections of the said Act. Provide sound legal advice to the company in accordance with the said Act above. **[10 Marks]**

(b) Define forensics sample in accordance with the National Forensics Act No. 2, of 2020 **[2 Marks]**

(c) Explain briefly, the implications of a cyber security expert operating without a license in accordance with the National Forensics Act No. 2 of 2020. **[3 Marks]**

(d) Finally, advice the Company based on the Evidence Act, Chapter 43, of the Laws of Zambia, especially to avoid any chance of recantation by the perpetrator **[5 Marks]**

Optional Questions

Instructions
Choose any four (4) more questions from Question Two to Question Seven (7).

Question Two [20 Marks]

1. The court has established that you can be an Amicus curia because they have realized that you can provide impartial, expert information to assist the court in understanding technical and electronic matters with regard to digital forensic relevant to a case proceeding at hand.
   (a) Explain what is meant by Data Minimization Principle to the court used in cybersecurity which should never be ignored when identifying and analysing data. Use of any available Act is encouraged but optional. **[2 Marks]**

(b) Give the court **two (2)** advantages and **two (2)** disadvantages of Data Minimization Principle **[4 Marks]**

(c) The court wants to understand the Anonymization and Pseudonymization techniques that you feel should have been used in Data Minimization as a principle in cybersecurity.

(i) Define Anonymization **[2 Marks]**

(ii) What is Pseudonymization? **[2 Marks]**

(iii) Mention **two (2)** advantages and disadvantages of anonymization and pseudonymization **[4 Marks]**

(d) Discuss ethical issues that you observed could have been neglected in the computer forensic that was carried out in terms of

(i) Non-Maleficence **[2 Marks]**

(ii) Beneficence **[2 Marks]**

(iii) Autonomy **[2 Marks]**

Question Three [20 Marks]

It is incumbent that the plaintiff must prove beyond reasonable doubt that the defendant committed the crime to the fact finders or coroner.

1. Define the following terms related to burden of proof;

(a) Burden of proof **[2 Marks]**

(b) Prima facie **[2 Marks]**

(c) Actus Reus **[2 Marks]**

(d) Mens Rea **[2 Marks]**

2. Discuss the differences between burden of production and burden of persuasion **[2 Marks]**

3. Explain the precise meaning of the term causation, also, what is meant by "but for" in a causation test. **[5 Marks]**

4. Distinguish "But for" and proximate cause in causation, giving precise example in each or possibly, case law in detail **[5 Marks]**

Question Four [20 Marks]

A Commercial bank would like to deploy qualified personnel in key positions in all its' ten (10) branches across the country. Before conducting planned face-to-face interviews, they engage you to help with digital screening by use of passive and active footprints of all the possible candidates.

1. Explain to the panel what is meant by Passive and Active footprints, giving an on-point example in each **[4 Marks]**

2. After further probing or investigation, you give advice to the panel that all those candidates that would make it to the next stage of the interviews, should now undergo computer forensics. One technique here is Cross Drive Analysis (CDA).

   (a) Describe Cross Drive Analysis (CDA) **[2 Marks]**

   (b) In your discussion as to why this technique is useful, highlight the importance of conducting a Cross Drive Analysis in terms of steganography detection, identifying hot drives, improving single drive analysis, live analysis, deleted file recovery, and social network identification. Give examples if possible. **[6 Marks]**

   (c) You have established that CDA uses statistical and lexical techniques to extract features from bulk data and identify patterns or anomalies in your investigation for proper decision making, understanding complex datasets, and predict future outcomes. Differentiate between statistical and lexical techniques in this context. **[2 Marks]**

   (d) Give or mention **two (2)** examples of software that could be used for Cross Drive Analysis (CDA) **[2 Marks]**

3. Highlight four challenges you are likely to face in your CDA investigations that you feel the panel should know in advance **[4 Marks]**

Question Five [20 Marks]

1. Define the following computer crimes, giving motivations by perpetrators and also, legal implications. Definitions from the Act is encouraged. .

   (a) Doxing **[3 Marks]**

   (b) Green graffiti **[3 Marks]**

   (c) Industrial espionage **[3 Marks]**

   (d) Data diddling **[3 Marks]**

2. Explain brief what you understand by 'bobby-trap' and how Message Digest Algorithm (MDA) 5 and SHA1 hashing algorithms could be used to deter a Bobby trap. **[8 Marks]**

Question Six [20 Marks]

1. The DPP has determined beyond reasonable doubt that a case must be opened and investigated in a crime believed to be murder, when friends of the diseased, 21, a student in a named University is alleged to have committed suicide. The Detective could only do much but needed an expert to crack this case using variables found at the scene. The Detective tips you as a digital forensic expert, that a mobile phone, belonging to the diseased, bank ATM cards and other seemingly, essential electronic devices were found on the crime scene. Use of

the extra material such as the Act in answering the questions below is encouraged.

(a) Discuss your answer by differentiating between formal (structured) and informal (unstructured) investigation in a table format **[5 Marks]**

(b) Outline **two (2)** possible digital forensics that could be carried out here **[2 Marks]**

(c) List and explain **three (3)** sure types of artifacts from other electronic devices found on the scene of crime that you would consider as a digital or computer forensics expert **[3 Marks]**

(d) Discuss **five (5)** steps you would carefully take to make sure that evidence collected, analysed and preserved is admissible in court. **[5 Marks]**

(e) Before trial, in a bench trial, it is said that investigators rely on tier of fact, and probative evidence ranging from multiple artifacts provided as evidence. Discuss in detail, what you understand by tier of facts, outlining the characteristics, and its importance as well in your explanation, further, explain briefly about probative of evidence **[5 Marks]**

Question Seven [20 Marks]

Chain of Custody often referred to as CoC, is a very important legal document.

1. Define chain of custody **[2 Marks]**

2. List and discuss **four (4)** important aspects or advantages of CoC **[4 Marks]**

3. Outline any **four (4)** challenges of CoC **[4 Marks]**

4. The Defendant has outlined something amiss in the CoC and decides to challenge evidence maintaining insistence that it is not supposed to be admissible in court. Discuss what could qualify for chain of custody not be admissible in the courts of Law in Zambia. Use of any underlisted Act of the Constitution of Zambia will attract more marks. **[4 Marks]**

5. Draft a sample of CoC and demonstrate how you would fill in the fields in the sample document you have just drafted. **[6 Marks]**

CHECK YOUR WORK BEFORE SUBMISSION!

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES

BACHELAOR OF SCIENCE IN CYBER SECURITY

SYSTEM VULNERABILITY ASSESSMENT

COURSE CODE: CYS 330

FINAL EXAMINATION

DURATION: Three hours (5 MINUTES TO READ THROUGH THE PAPER)

INSTRUCTIONS

1. There are **seven** questions in this paper. **Question One Part A** and **Part B are** compulsory. Answer any **three (3)** more questions from Question **Two** to Question **Seven**

2. The examination paper carries a total of **60 marks**. Marks are allocated at the end of each question accordingly.

3. Candidates are **NOT** permitted to use any type of calculator in this examination. use of any other extra materials other than what has been permitted will be considered as examination malpractice against the University's examination ethical conduct.

4. Make sure to write all the necessary details on the answer sheet provided. Use of a neat and clear handwriting is encouraged.

5. **Candidates must not turn this page until told to do so by the Supervisor of this examination**

Question One Part A [23 Marks]

Instructions: Show all your working to earn marks.

1. Computational calculations help IT professionals to explicitly explain an overflow as a vulnerability. Add the following numbers in one's compliment. Determine whether an overflow has occurred.

(a) -55 and (-47) **[3 Marks]**

(b) 98 and 77 **[3 Marks]**

2. Add the following numbers in two's compliment. Determine whether an overflow has occurred

(a) -88 and (-72) **[3 Marks]**

(b) 81 and 81 **[3 Marks]**

3. Subtract the following numbers in two's compliment. Determine whether an overflow has occurred

(a) 65 – (-23) **[3 Marks]**

(b) 11 – 9 **[2 Marks]**

4. Subtract the following numbers in one's compliment. Determine whether an overflow has occurred

(a) 33 – 27 **[3 Marks]**

(b) 29 – (-25) **[3 Marks]**

PART B [13 Marks]

1. Mitigation and remediation are a must in the field of computing especially cybersecurity for both prevention and aftermath of a vulnerability. To help with these two vital aspects of your field, PERT chart comes in handy. Consider the following data given and answer the questions that follow;

Activities	Optimistic (O)	Most Likely (M)	Pessimistic (P)
1 – 2	1	2	3
1 – 3	5	6	7
1 – 4	3	5	7
2 – 5	5	7	9
3 – 5	2	4	6
5 – 6	4	5	6
4 – 7	4	6	8
6 – 7	2	3	4

(a) Draw a network diagram using the above information **[3 Marks]**

(b) Calculate the expected Variance (V) of each activity **[4 Marks]**

(c) Calculate the Standard Deviation (SD) of each activity **[4 Marks]**

(d) Determine the expected duration for each activity **[4 Marks]**

(e) Determine the expected critical path variance **[2 Marks]**

Optional Questions

Instructions
Choose any three (3) more questions from Question Two to Question Seven (7).

Question Two [20 Marks]

1. vulnerabilities in any network are unwanted and organisations would do anything possible to employ personnel or professional to take care of vulnerabilities in their system.

(a) Discuss **three (3)** out of many Moden security threats that organisations endeavour to overcome nowadays **[3 Marks]**

(b) Mention and explain briefly, **three (3)** components of information security ensured by cryptography **[3 Marks]**

(c) Malware is one vulnerability underlisted to cause so many unwarranted problems. Give and explain briefly, two precise primary methods in which malware could be mitigated. **[2 Marks]**

(d) Describe **two (2)** ways on how the organisation could mitigate the impact of DDoS attacks **[2 Marks]**

2. Implementation of AAA in an organisation's network is technically encouraged.

(a) Explain how implementation of AAA in a network can help secure a network in an organisation **[2 Marks]**

(b) Mention and explain briefly, at least **three (3)** potential drawbacks of using AAA in a network **[3 Marks]**

(c) Differentiate in a table format, any **five (5)** differences between RADIUS and TACACS+ deployment tradeoffs in AAA **[5 Marks]**

Question Three [20 Marks]

1. Web forms and web applications commonly use Structured Querry Language otherwise known as SQL in querying databases.

(a) It is reported to you that a web application in your website, is failing to sanitize user input, in a login form. Describe an example payload you may try to use to test for SQL injection (SQLi) **[3 Marks]**

(b) Explain briefly how Time-Based SQL injection can be used to infer information from a database **[2 Marks]**

(c) Given a statement below,

SELECT* FROM Users WHERE Username = ' ' OR '1' = '1';

(i) Explain briefly, why this may be vulnerable to SQLi **[2 Marks]**

(ii) Describe the significance of the payload 'OR' '1' in SQLi **[2 Marks]**

(iii) Describe the UNION – Based SQL injection works **[2 Marks]**

(d) Give and explain **three (3)** common types of SQL injection attacks **[3 Marks]**

2. One way to eradicate SQLi is using parameterized queries. Or prepared statements.

(i) Explain briefly, what is meant by parameterized or prepared statements in SQL. **[2 Marks]**

(ii) Discuss how parameterized queries may help to prevent SQL injection attacks **[2 Marks]**

(iii) Name at least **two (2)** other more security best practices to defend against SQL injection attacks **[2 Marks]**

Question Four [20 Marks]

1. Another vulnerability which tends to be overlooked and underrated is the hardware trojan

(a) Define hardware trojan in your own words and explain how it differs with the software malware **[2 Marks]**

(b) Describe **two (2)** main types of payloads that a hardware trojan can carry **[2 Marks]**

(c) Give and describe **two (2)** common trigger mechanisms for hardware trojan as a vulnerability **[2 Marks]**

(d) Explain how a hardware trojan could cause physical damage to integrated circuits (ICs) **[2 Marks]**

2. Integrated Circuits (ICs) use logic gates such as AND gate, OR gate, NOT gate, NAND gate, EXOR gate, XOR gate, NOR gate and XNOR gate. .

(a) Represent the following logic gates in form of symbol, Boolean expression and Truth table.

(i) OR gate **[3 Marks]**

(ii) NOT gate **[3 Marks]**

(iii) AND gate **[2 Marks]**

(b) Discuss the potential consequences of hardware trojan insertion in critical infrastructure systems such as Military **[2 Marks]**

(c) Explain briefly, how supply chain globalization increases the risk of trojan hardware insertion **[2 Marks]**

Question Five [20 Marks]

1. The following are pieces of data for your consideration

Activities	Duration
1 – 2	13
1 – 3	12
2 – 4	2
3 – 4	8
2 – 5	15
4 – 5	2

(a) Draw a network diagram from the data given above **[4 Marks]**

(b) Determine the Critical Path (CPM) of the project **[2 Marks]**

(c) Find the project duration in days **[2 Marks]**

(d) Calculate the;

(i) Total float (TF) **[3 Marks]**

(ii) Free float (FF) **[3 Marks]**

(iii) Independent Float (IND F) **[3 Marks]**

(iv) Interfering Float (INT F) **[3 Marks]**

Question Six [20 Marks]

1. Cross-Site Request Forgery (CSRF) is a web security vulnerability common according to Common Vulnerability Exposure.

(a) Describe CSRF using short notes **[4 Marks]**

(b) Explain briefly, how APIs as well as forms could be secured to prevent CSRF in a website **[2 Marks]**

(c) Discuss **four (4)** measures that could be put in place to mitigate CSRF by a website of a big organisation **[4 Marks]**

(d) Differentiate clear CSRF and XSS in terms of the following aspects;

(i) Attack goal **[2 Marks]**

(ii) Session requirement **[2 Marks]**

(iii) User interaction **[2 Marks]**

(iv) Attack vector **[2 Marks]**

(v) Data access **[2 Marks]**

Question Seven [20 Marks]

1. Common Vulnerability Exposure (CVE) is a publicly available catalog and reference system that identifies and standardizes known cybersecurity vulnerabilities and exposures in both software and hardware managed by MITRE cooperation.
   (a) Discuss the difference between Common Vulnerability Exposure (CVE) and Common Weakness Enumeration (CWE) **[2 Marks]**

   (b) Explain how, as a security professional, you would use CVE in vulnerability assessment and penetration testing in your organisation **[2 Marks]**

   (c) Briefly explain, how CVE contribute to prioritizing patch management in your organisation. **[2 Marks]**

   (d) A recent CVE describes a remote code execution vulnerability in a widely used server software. Describe steps you would take as a professional in an organisation to mitigate the risk posed by this CVE **[3 Marks]**

2. Describe the role of Common Vulnerability Scoring System (CVSS) in relation to CVEs **[4 Marks]**

3. Explain how CVSS base, temporal, and environmental scores help in vulnerability prioritization **[3 Marks]**
4. Explain briefly, what each colour code below means in CVSS;
   (a) Red **[1 Mark]**

   (b) Orange **[1 Mark]**

   (c) Green **[1 Mark]**

   (d) Yellow **[1 Mark]**

CHECK YOUR WORK BEFORE SUBMISSION!

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCES

CSY331 – WIRELESS SECURITY
2025 SESSIONAL EXAMINATIONS

Date: 4th November 2025

Instructions :

1. Time allowed is **three (3) hours**
2. There are **Seven (7) Questions** in this paper.
3. You are required to answer any **Five (5)** questions.
4. Total Marks: **100**.

Question 1 [20 Marks]

Wireless communication allows data to be transmitted without the need for physical cables, using electromagnetic waves. This technology has transformed the way we connect and communicate across distances.

a) List and Describe two importance of wireless communication in modern technology. **[4 Marks]**

b) Compare wired and wireless networks in terms of speed, reliability, and mobility. **[3 Marks]**

c) Discuss the cost and complexity of setting up wired and wireless networks. **[4 Marks]**

d) Give one advantage and one disadvantage of Wireless Personal Area Networks (WPANs) in terms of range and speed. **[4 Marks]**

e) Discuss how the lack of a physical medium affects the reliability of data transmission in wireless networks. **[3 Marks]**

f) Compare Wireless Metropolitan Area Networks (WMANs) and Wireless Wide Area Networks (WWANs) in terms of coverage and security. **[2 Marks]**

Question 2 [20 Marks]

The rise of wireless technology has opened up many opportunities for innovation, including the widespread use of wireless data services and public connectivity.

a) Describe three common applications of wireless technology in everyday activities. **[3 Marks]**

b) Describe how wireless hotspots provide public internet access in locations like airports and cafes. **[2 Marks]**

c) Discuss two main challenges faced by wireless networks and suggest potential solutions. **[4 Marks]**

d) What are the two main characteristics of WPANs? **[2 Marks]**

a) How does WPAN differ from a Wireless Local Area Network (WLAN),give two difference. **[4 Marks]**

b) Describe the concept of a "piconet" and how Bluetooth devices form a network. **[3 Marks]**

c) What are the roles of master and slave devices in a piconet? **[2 Marks]**

Question 3 [20 Marks]

Communication is done by transmission media which can either be guided or unguided, transmission.

a) What is the difference between guided and unguided transmission? **[2 Marks]**
b) Describe the three types of wireless transmission media: Radio waves, Microwaves, and Infrared? **[6 Marks]**
c) Give two applications of radio wave transmission? **[2 Marks]**
d) Discuss two disadvantages of radio wave transmission. **[4 Marks]**
e) What is infrareds (IR) transmission and give two applications of InfraRed. **[6 Marks]**

Question 4 [20 Marks]

Wireless networks are exposed to several threats because signals travel through the air, making interception and disruption easier than in wired systems.

a) Define eavesdropping in wireless networks and state two practical countermeasures. **[3 Marks]**
b) Differentiate spot, sweep, and barrage jamming. **[3 Marks]**
c) Give and Explain one effective anti-jamming technique. **[2 Marks]**
d) What is Radio Frequency (RF) interference? **[2 Marks]**
e) Give two common sources of Radio Frequency (RF) and one effect on network performance. **[6 Marks]**
f) Explain spoofing and propose one mitigation. **[4 Marks]**

Question 5 [20 Marks]

Even when payloads are encrypted, attackers can analyze metadata (timing, sizes, addresses) to infer sensitive patterns—one can also exploit protocol/crypto weaknesses such as KRACK.

a) Define traffic analysis (TA) and briefly contrast it with payload eavesdropping. **[3 Marks]**
b) Describe two Traffic Analysis techniques/tools **[3 Marks]**
c) A rogue device pretends to be the official Wi-Fi router by copying its MAC address. What is this attack? **[2 Marks]**
d) A hacker floods all wireless channels in an area, causing total signal disruption. What jamming type is this? **[2 Marks]**

e) A mobile device reconnects to a Wi-Fi network quickly by skipping full authentication. What handshake is used? **[2 Marks]**

f) A company secures its old mobile WAP devices with a protocol designed for low bandwidth. What is this protocol? **[3 Marks]**

g) You are setting up authentication using port-based network access control on Wi-Fi. Which protocol do you use? **[3 Marks]**

h) The server responsible for authenticating users in an enterprise Wi-Fi setup is called what? **[2 Marks]**

Question 6 [20 Marks]

Wi-Fi security has evolved from WEP to WPA/WPA2 and now WPA3, alongside standards like IEEE 802.11i and 802.1X, plus the 4-way handshake for key establishment.

a) Compare WEP and WPA2-AES/CCMP in terms of ciphers used and key/IV handling, and state why WEP is insecure today. **[4 Marks]**

b) Explain the 4-way handshake? **[3 Marks]**

c) What are the two messages and two keys exchanged during the handshake. **[4 Marks]**

d) Explain two key improvements in WPA3 and what security properties they add. **[3 Marks]**

e) Define supplicant, authenticator, and authentication server (RADIUS). **[6 Marks]**

Question 7 [20 Marks]

WTLS adapts TLS for wireless/WAP environments with constrained bandwidth and device resources, offering integrity, privacy, authentication, and handshake variants (full vs. abbreviated).

a) List and briefly explain three security functions WTLS provides.**[3 Marks]**

b) Distinguish a full handshake from an abbreviated handshake **[4 Marks]**

c) List and explain any three types of Denial of Service (DOS). **[6 Marks]**

d) Differentiate between a threat and security breach in terms of timing, action and impact.**[6 Marks]**

e) A secure Wi-Fi network requires AES encryption with CCMP. Which protocol satisfies this?**[1 Mark]**

END

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM 2025

Course Title: Fraud and Detection Technologies

Course Code: CYS 339

Duration: 3HRS

Total Marks: 60 Marks

General Instructions to Candidates:

1. Answer **Question 1** and **Question 2** (Compulsory) and **any two** from Questions 3, 4, and 5.
2. No unauthorised materials are allowed.
3. You are allowed to use calculators (but programmable calculators are not permitted)
4. Start each answer on a new page.
5. Write clearly and neatly.

Note: Any form of examination malpractice will result in disciplinary action.

SECTION A (Compulsory)

QUESTION 1

A cybersecurity team is analysing the effectiveness of their new intrusion detection system (IDS) over two quarters.

In Quarter 1 (Q1) the budgeted security incident response cost $50,000 while the actual cost was $65,000 whilst in Quarter 2 (Q1) the budgeted security incident response cost was $55,000 with the actual cost being $48,000. The total number of alerts in Q2 was 12,000 with the number of true positive alerts (actual threats) being 960

a) Calculate the cost variance for both Q1 and Q2. For each, state whether it is a favorable or unfavorable variance and explain what this means in the context of cybersecurity spending. [6 marks]

b) Calculate the False Positive Ratio for the IDS in Q2. [3 marks]

c) Based on your calculations, advise the Chief Cybersecurity Officer on two reasons why relying solely on these financial ratios and variances might give an incomplete picture of the IDS's performance. [6 marks]

QUESTION 2

a) Define Gap Analysis and explain its importance in fraud detection. [4 Marks]

b) Outline the five (5) key steps in conducting a gap analysis for fraud prevention in an organisation. [5 Marks]

c) A company's fraud detection system has a high false-positive rate. Using gap analysis, suggest three (3) improvements to reduce false alerts. [6 Marks]

SECTION B (Answer any two)

QUESTION 3

a) Compare qualitative and quantitative data analysis in fraud detection by providing two (2) strengths and two (2) weaknesses for each. [6 Mark]

b) Explain how behavioral profiling can detect fraudulent transactions in banking. [5 Marks]

c) A fraud analyst is investigating an unusual spike in refund requests. Recommend two quantitative and two qualitative techniques to determine if this is fraud. [4 Marks]

QUESTION 4

a) Briefly explain the four (4) stages of the OLAF Approach in fraud investigations. [4 Mark]

b) How can link analysis (under the "Follow" stage) help uncover a vendor fraud scheme? [5 Marks]

c) Discuss two (2) challenges investigators may face when applying the OLAF approach in digital forensics. [6 Marks]

QUESTION 5

a) Explain three (3) considerations when selecting between generic and specific fraud detection tools. [6 Marks]

b) Describe how critical thinking and logical reasoning help in formulating fraud hypotheses. [4 Marks]

c) A company suspects payroll fraud. Outline a step-by-step data analysis plan to investigate. [5 Marks]

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of information and communication technology

FINAL EXAM

Course Title: CYBERCRIME INVESTIGATION AND FORENSICS 2

Course Code: CYS 340

Instructor Name: MR NGOSA GATHAM

Moderator Name: .....

Date: .....

Duration: 3HRs

Total Marks: 60

General Instructions to Candidates:

1. Answer question 1 and any other three
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and legibly.

Exam Instructions:

Any student that will be caught with foreign material, copying or behaving in a manner viewed as examination malpractice/misconduct, will be subjected to disciplinary hearing or disqualification.

Question 1

A malware sample injects itself into system processes and hides from disk scans.

a) As a forensic analyst, Explain step-by-step the process of analyzing volatile memory in this case using memory forensics. (3 marks)
b) Discuss four unique conditions where only memory forensics applies (4 marks)
c) Describe at least five main formats of memory data essential for forensic investigations. (5 marks)
d) Discuss three methods of memory data acquisition that you may opt to use in this case (3 marks)

Question 2

During a cyber-attack investigation, you are tasked with analyzing a seized hard drive that contains deleted files suspected to be related to illegal activities

a) Explain the possible types of deletion the suspect could have used. (3 marks)
b) Outline the typical steps involved in file carving. (6 marks)
c) Discuss challenges faced during file reconstruction like this one and propose solutions to overcome such. (6 marks)

Question 3

Investigators are asked to analyze a cyber-attack in a hybrid cloud model.

a) What challenges are they likely to face, and what measures should they adopt (6 marks)
b) With the aid of a diagram, discuss cloud service models from a forensic perspective (3marks)
c) Compare and contrast cloud forensics to traditional digital forensics(6 marks)

Question 4

1. A hacker used a rootkit to maintain persistence in a victim's machine
   a) As a forensic analyst, Describe how malware forensics can uncover such hidden threats?(5 marks)
   b) Identify five types of malware common in forensics, describe their characteristics and how they can be detected. (5 marks)
   c) Describe three proactive measures to protect systems from malware attacks (3 marks)

d) With clear examples, distinguish signature-based from heuristic-based malware detection techniques. (2 marks)

Question 5

You are asked to present forensic evidence in court.

a) Explain how adherence to digital forensic regulations ensures admissibility. (4 marks)
b) Explain Locard's Exchange Principle and its significance in digital forensics(2 marks)
c) Discuss at least five organizations that govern digital forensics internationally (5 marks)
d) If a fraud case involving online banking has been reported. As a cyber-forensic investigator (CFI), describe your roles in solving this case. (4 marks)

Question 6

An investigator finds multiple multimedia files that have been tampered with in an online fraud case

a) Explain how multimedia forensics helps in establishing the integrity of evidence (5 marks)
b) Describe methods used to analyze images, audio, and video files (3 marks)
c) Discuss why understanding the five elements of multimedia aids in collecting reliable digital evidence. (5marks)
d) Identify and describe two common cybercrime investigation tools used multimedia forensics (2 marks)

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM

Program: Bachelor of Science in Cyber Security

Course Title: Mobile Device and Security and Forensic

Course Code: CYS 425

Date: 13TH November 2025

Duration: 3HRS

Total Marks: 100

General Instructions to Candidates:

1. Answer questions 1 and 2 and any other 3 three questions.
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

[QUESTION 1]

You are a digital forensics expert with the Zambia Police Service's Cybercrime Unit. You have been called to a fraud investigation where the suspect's smartphone is a key piece of evidence. The suspect allegedly used the device to communicate with accomplices and transfer illicit funds.

(a) List FOUR different types of data commonly found on a mobile device that are crucial for a forensic investigation. (4 Marks)

(b) Explain TWO specific challenges you might face when attempting to extract data from this smartphone, relating to legal or ethical aspects. (4 Marks)

(c) Describe the first THREE critical steps you would take immediately upon receiving the mobile device to preserve the integrity of the evidence, starting from physical seizure.

(6 Marks)

(d) The suspect's lawyer argues that extracting data from the cloud (e.g. Google Drive backups) violates their client's privacy beyond the scope of the warrant for the physical device.

i. Analyze the validity of this challenge. (3 Marks)

ii. Create a checklist of three points you would provide to the legal team to justify the need for cloud data acquisition in this investigation. (3 Marks)

[QUESTION 2]

A suspect in a fraud case uses a high-end Android phone with the latest operating system. Initial attempts at a logical acquisition have failed due to the device's strong security features.

(a) What is the primary purpose of the Secure Boot process in a modern mobile device?

(2 Marks)

(b) Name two encryption mechanisms used in mobile devices. (2 Marks)

(c) Explain the legal implications of extracting data from a mobile device without consent or warrant. (2 Marks)

(d) Differentiate between Full Disk Encryption (FDE) and File-Level Encryption. (4 Marks)

(e) Outline the key components of a forensic report for a mobile device investigation. Include examples of the information required in each section. (10 Marks)

[QUESTION 3]

You are presenting your findings from a mobile forensics investigation in a high-profile court case. The defense counsel is challenging the integrity of your evidence, claiming the chain of custody was broken when the device was transported from the police station to your lab.

(a) What is the fundamental purpose of maintaining a Chain of Custody in a digital forensic investigation? (2 Marks)

(b) Explain the importance of hashing (using algorithms like SHA-256) in the evidence handling process. What does it prove about the data you have extracted? (4 Marks)

(c) During your testimony, you are asked what specific steps you took to minimize interaction with the device upon receipt. Describe THREE forensic best practices you followed from the moment you received the evidence bag. (6 Marks)

(d) The judge asks you to demonstrate that the evidence is authentic and reliable.
i. Evaluate the potential consequences of not having a properly documented chain of custody form. (4 Marks)
ii. One of the defense lawyers powers on a seized phone to "see if it works." Critique this

action by explaining TWO specific types of evidence that could be altered or destroyed by this mistake. (4 Marks)

ii. Create a simple, 5-step procedural checklist for field agents to follow when seizing a mobile device, ensuring evidence integrity from the moment of seizure. (4 Marks)

[QUESTION 4].

Your digital forensics unit has a limited budget. You must decide between investing in a new commercial tool like Cellebrite UFED or relying on a suite of open-source tools like Autopsy.

(a) Define Mobile device forensics and explain its significance in criminal investigations. (4 Marks)

(b) Name ONE widely used commercial mobile forensic tool and ONE popular open-source alternative. (2 Marks)

(c) Compare open-source and commercial forensic tools by listing TWO advantages of each. (4 Marks)

(d) A specific case requires the extraction of data from a rare Chinese-manufactured Android phone.

i. Which type of tool (Commercial or Open-Source) would likely offer better support for this device, and why? (3 Marks)

ii. Regardless of your choice, what is one crucial step you must take to validate the findings from your forensic tool? (3 Marks)

(e) The head of your unit asks for a justification for the high cost of a commercial tool license.

i. Evaluate the situation by arguing FOR the purchase of the commercial tool, focusing on two key benefits that would justify the expense for a law enforcement context. (4 Marks)

[QUESTION 5].

In a child exploitation case, the suspect's iPhone was seized, but critical evidence is believed to be stored in their iCloud account and synced with an Apple Watch.

(a) What are TWO major challenges forensic investigators face when dealing with evidence stored in the cloud? (2 Marks)

(b) Explain the concept of data jurisdiction and why it complicates cloud forensics investigations. (4 Marks)

(c) Describe the process of legally obtaining data from the suspect's iCloud account. (4 Marks)

(d) The suspect's Apple Watch is a potential source of evidence.
i. Analyze the specific types of forensic data you might extract from the Apple Watch (an IoT device) that could corroborate or expand upon evidence from the iPhone. (6 Marks)
ii. Create a checklist of four questions you would need to answer before beginning the acquisition of data from the Apple Watch. (4 Marks)

[QUESTION 6].

You are a forensic expert hired by a defense attorney. The prosecution's case relies heavily on evidence extracted from the defendant's phone. You are reviewing the methods used by the police forensics team.

(a) The forensic report states the tool used was "Cellebrite UFED." Why is it not sufficient for the report to merely state the tool used? What additional information about the process is required to establish authenticity? (4 Marks)

(b) The defendant claims they did not give consent for their phone to be searched, and there is no search warrant in the evidence file.
i. What legal principle does this potentially violate? (3 Marks)
ii. What would be the likely consequence for the evidence in court? (3 Marks)

(c) During your review, you discover that the police examiner accessed personal photos and messages that were unrelated to the case.

i. Evaluate this action from an ethical perspective, referring to the principle of minimization. (5 Marks)

ii. Create a "Code of Conduct" for mobile forensic examiners that would help prevent such ethical breaches. (5 Marks)

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of information and communication technology

Final exam

Course Title: CLOUD COMPUTING AND SERVICES

Course Code: CYS 440

Instructor Name: MR NGOSA GATHAM

Moderator Name: .....

Date: .....

Duration: 3HRs

Total Marks: 60

General Instructions to Candidates:

1. Answer question 1 and any other three
2. No unauthorized materials are allowed
3. No electronic devices allowed unless specified.
4. Start each answer on a new page.
5. Write clearly and legibly.

Exam Instructions:

Any student that will be caught with foreign material, copying or behaving in a manner viewed as examination malpractice/misconduct, will be subjected to disciplinary hearing or disqualification.

Question 1

Kapasa Makasa University plans to migrate its ICT services to the cloud to improve efficiency and service delivery. The management board is seeking clarity on the benefits and challenges of adopting cloud computing.

a) Clearly explain six benefits the university is likely to gain from adopting cloud computing services (3 marks)

b) Identify two potential challenges the university may encounter during and after cloud adoption, propose possible solutions to combat them. (4 marks)

c) State and briefly explain three cloud service models that the university can choose from, indicating one possible application of each in a university setting. (6 marks)

d) Among deployment models you have stated above, which one best suit the university's needs if it wants to maintain control over sensitive academic records but still use public resources for email and storage? Justify your choice. (2 marks)

Question 2

A startup company is considering migrating its on-premises infrastructure to the cloud to improve scalability and reduce costs. They are evaluating virtualization options to optimize resource utilization.

a) Explain what virtualization is and its role in cloud computing. (2 marks)

b) Discuss three benefits of virtualization to startups like this one. (3 marks)

c) Describe different types of virtualization with real-world examples relevant to the startup's needs. (6 marks)

d) With the aid of a diagram, distinguish bare metal from hosted hypervisor implementation in virtualization. (4 marks)

Question 3

a) Mention and explain five key components of a data center. (5 marks)

b)) Clearly explain five factors to consider when establishing a new data center. (5 marks)

c) Why is power backup critical for a data center? (2 marks)

d) If you were asked to establish a data center, where would you recommend it to be located and why? (3 marks)

Question 4

a) Describe how to create a root account on AWS (4 marks)

b) Which cloud provider would be best for Kapasa Makasa University which is planning to store massive amounts of research data? Justify. (2 marks)

c) List and explain five factors to consider when choosing a cloud provider. (5 marks)

d) Discuss two similarities shared by AWS and Azure. (4 marks)

Question 5.

MTN Africa is deploying a cloud solution for its global operations. The company's cloud ecosystem involves multiple actors, including the cloud provider, internal IT teams, and third-party auditors.

a) Iilustrate the roles of Cloud Service Providers, Cloud Consumers, Cloud Brokers, and Cloud Auditors in this scenario. (8 marks)

b) Explain how these actors collaborate to ensure secure and reliable cloud service delivery. (4 marks)

c) Discuss the importance of trust, compliance, and transparency among these actors in maintaining cloud security. (3 marks)

Question 6.

Chinsali General Hospital is considering cloud computing to digitize patient records and manage telemedicine services.

a) Which service model is most suitable for hosting email services? Why? (3 marks)

b) With clear examples, explain how cloud service composition and quality of service will enhance service delivery to the patients at the hospital. (4 marks)

c) How will the hospital management benefit from the business-value chain in the cloud ecosystem. (5 marks)

d) Discuss three privacy and security measures that should be put in place. (3 marks)

KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

Department of Information and Communication Technology

FINAL EXAM

Course Title: Server Management and Firewall

Course Code: CYS 471

Date: November 2025

Duration: 3HRS

Total Marks: 100

General Instructions to Candidates:

1. Answer questions 1 and 2 and any other THREE questions.
2. No unauthorized materials are allowed
3. No electronic devices are allowed.
4. Start each answer on a new page.
5. Write clearly and neatly.

Please Note: *Students that are caught with foreign material, copying or behave in any manner that is viewed as examination malpractice/misconduct will be subjected to a disciplinary hearing.*

[QUESTION 1]

A. Define "Risk Treatment" in the context of information security management and list **THREE** common risk treatment options. [3 Marks]

B. An organization identifies a vulnerability with an estimated likelihood of occurrence of 60% and an impact value of ZMK 50,000. Calculate the risk value using the formula Risk = Likelihood × Impact. Show your working. [4 Marks]

C. Compare and contrast the ISO/IEC 27001 and NIST Cybersecurity Framework in terms of their structure, core components, and typical use cases in an organizational context. [7 Marks]

D. You are the security manager at a university that has just suffered a ransomware attack affecting student records. Outline the key steps you would take in the first 24 hours, referencing the incident response lifecycle. [6 Marks]

[20 Marks]

[QUESTION 2]

A. Briefly explain the principle of Least Privilege and why it is important in access control systems. [3 Marks]

B. A system uses Role-Based Access Control (RBAC). There are 3 roles: Admin, Editor, and Viewer. An Admin can read, write, and execute; an Editor can read and write; a Viewer can only read. If a user is assigned the Editor role, list all the permissions they would have. [4 Marks]

C. Compare Signature-Based IDS and Anomaly-Based IDS in terms of how they detect threats, their advantages, and their limitations. Use a table for your comparison. [7 Marks]

D. A company's web server is experiencing repeated login attempts from an unknown IP address. Describe how an Intrusion Prevention System (IPS) could be configured to respond to this threat. [6 Marks]

[20 Marks]

[QUESTION 3]

A. Define Server Hardening and state two key objectives of the process. [3 Marks]

B. A default-deny firewall policy is in place. Write two firewall rules that would allow (1) HTTP traffic on port 80 and (2) SSH traffic on port 22 from any source. [4 Marks]

C. Explain the role of a Next-Generation Firewall (NGFW) and discuss how it differs from a traditional stateful inspection firewall. [7 Marks]

D. You are tasked with setting up a new file server for a small business. Describe three server hardening measures you would implement before making the server live. [6 Marks]

[20 Marks]

[QUESTION 4]

A. What is the primary purpose of a Virtual Private Network (VPN) and what security service does it primarily provide? [3 Marks]

B. A remote user needs to connect to the company's internal network using a VPN. List three authentication factors that could be used as part of a multi-factor authentication (MFA) process for the VPN login. [4 Marks]

C. Compare IPSec and SSL/TLS VPNs in terms of their typical use cases, layers of operation, and security strengths. [7 Marks]

D. An organization with multiple branch offices wants to securely connect their networks. Recommend a VPN type and describe one key security best practice they should implement. [6 Marks]

[20 Marks]

[QUESTION 5]

A. What is the primary security goal of the Bell-LaPadula model, and what are its two main rules? [3 Marks]

B. Using the Take-Grant model, if subject S1 has the "Grant" right over object O1, and subject S2 has the "Take" right from S1, explain what permission S2 can acquire regarding O1. [4 Marks]

C. Compare the Biba Integrity Model and the Clark-Wilson Model in terms of their focus, key principles, and typical application environments. [7 Marks]

D. A bank wants to ensure that no single employee can initiate and approve a financial transaction. Which security model would you recommend, and how would it be applied? [6 Marks]

[20 Marks]

[QUESTION 6]

A. Define Cross-Site Scripting (XSS) and name two types of XSS attacks. [3 Marks]

B. A web application has a login form vulnerable to SQL Injection. Write an example of a malicious input that could be used to bypass authentication. [4 Marks]

C. Describe the Secure Software Development Lifecycle (SDLC) and explain how security is integrated into at least three of its phases. [7 Marks]

D. You are reviewing a web application that stores user passwords in plaintext. Identify the vulnerability and recommend two specific measures to address it. [6 Marks]

[20 Marks]

[QUESTION 7]

A. What is the purpose of Patch Management in operating system security? [3 Marks]

B. A server has 5 services running, but only 3 are necessary for its role as a web server. Calculate the percentage reduction in attack surface if the unnecessary services are disabled. Show your working. [4 Marks]

C. Discuss the importance of log monitoring and auditing in server security. What types of events should be logged, and how can logs be protected from tampering? [7 Marks]

D. You are hardening a Linux web server. Describe three specific OS-level hardening steps you would take beyond applying patches. [6 Marks]

[20 Marks]