STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

My Portfolio for the Subject
Information Assurance and Security

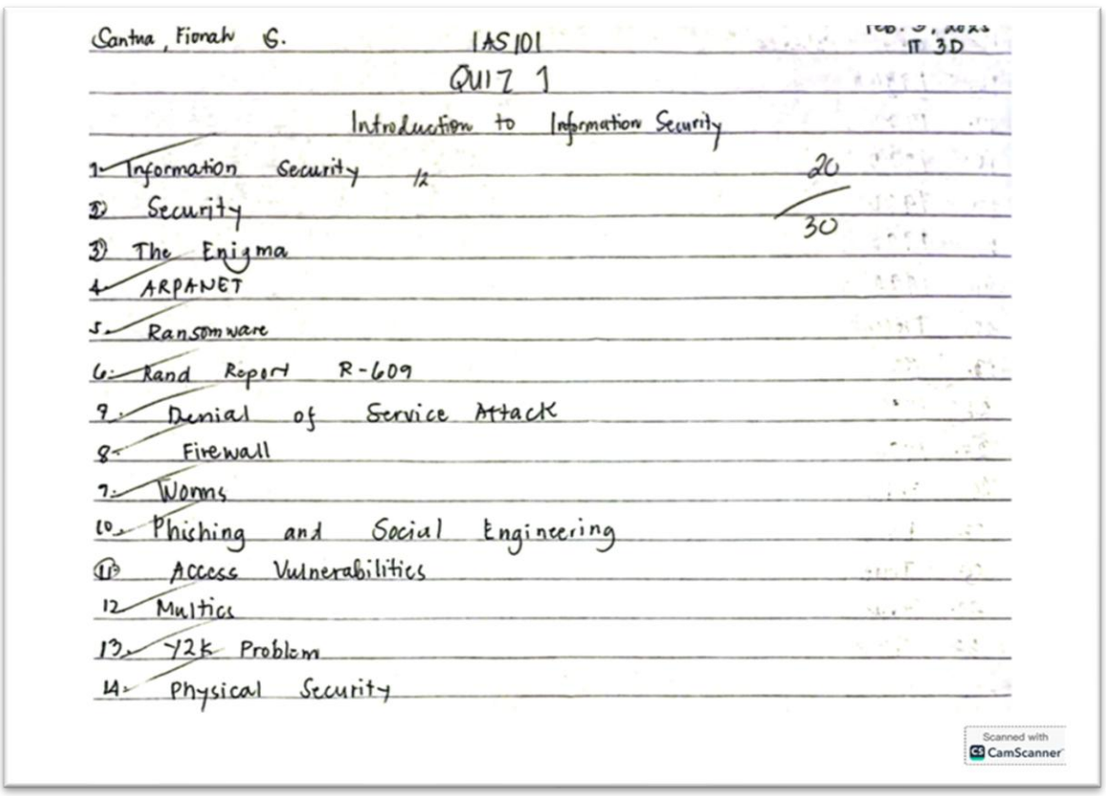
SUBMITTED BY: FIONAH S. SANTUA | 3D
PRESENTED TO: NAHUM QUIROS

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

TABLE OF CONTENTS

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 1

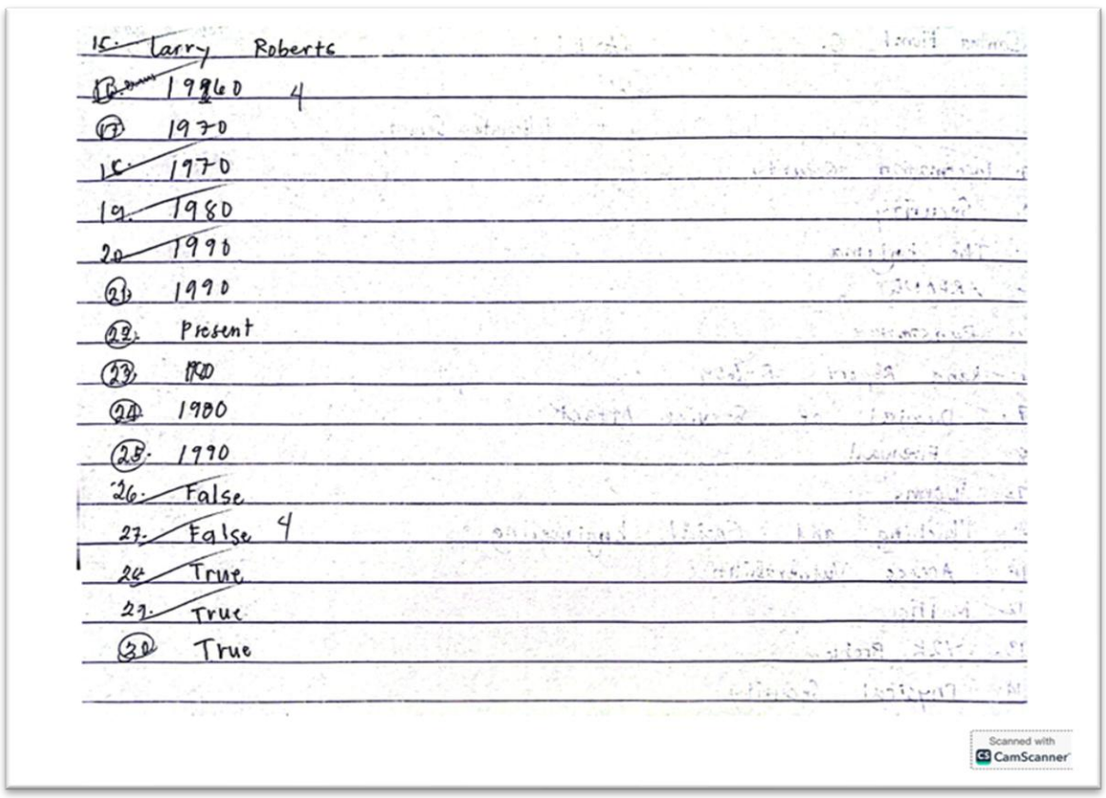


Cantua, Fionalv G. IAS101 IT 3D
QUIZ 1
Introduction to Information Security

1. Information Security 1/2
2. Security
3. The Enigma
4. ARPANET
5. Ransomware
6. Rand Report R-609
7. Denial of Service Attack
8. Firewall
9. Worms
10. Phiching and Social Engineering
11. Access Vulnerabilities
12. Multics
13. Y2k Problem
14. Physical Security

20/30

Scanned with CamScanner

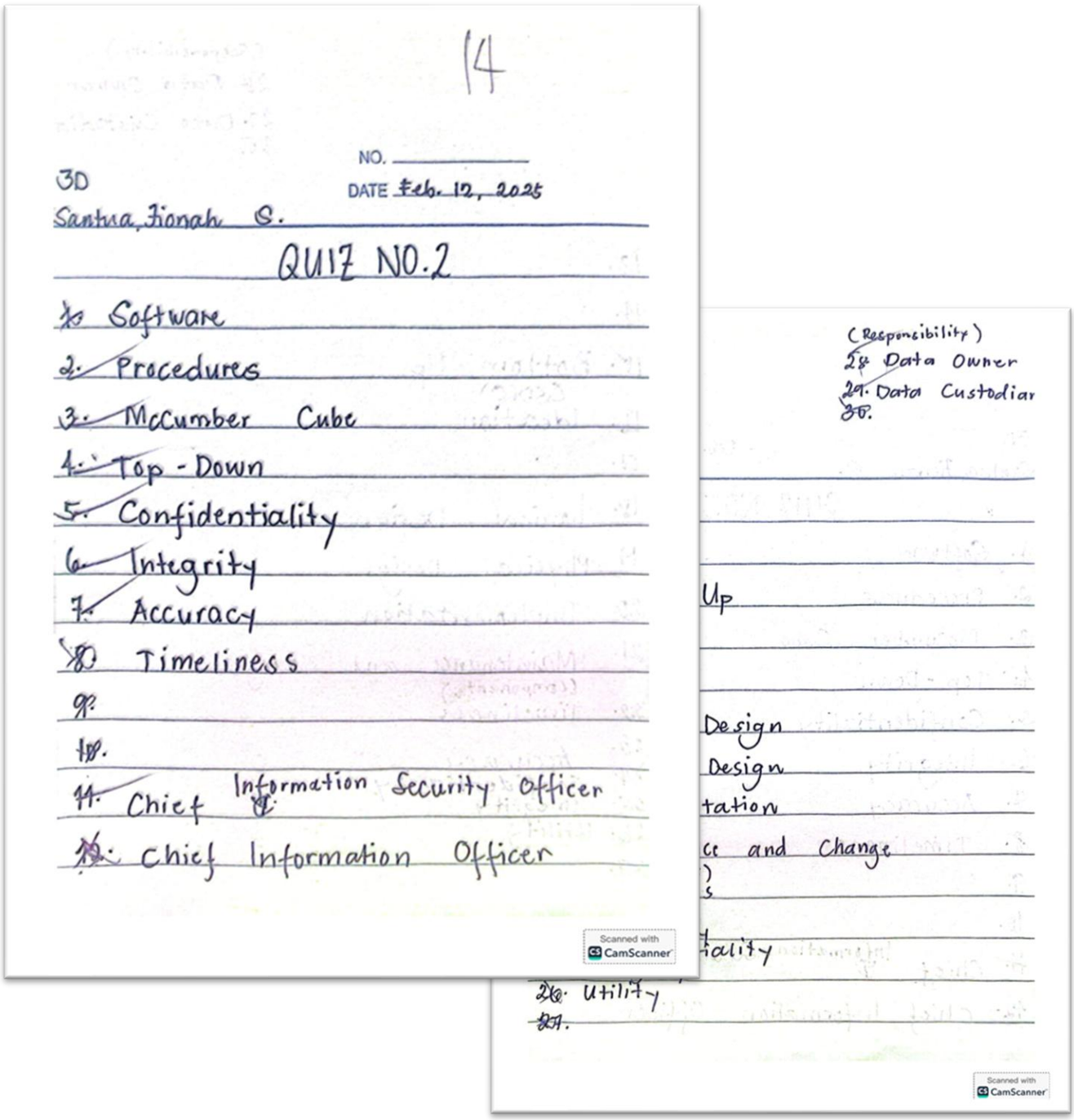


15. Larry Roberts
16. 19960 4
17. 1970
18. 1970
19. 1980
20. 1990
21. 1990
22. Present
23. 1900
24. 1980
25. 1990
26. False
27. False 4
28. True
29. True
30. True

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 2



14

NO. _____
3D DATE Feb. 12, 2025
Santua, Fionah S.

QUIZ NO.2

1. Software
2. Procedures
3. McCumber Cube
4. Top - Down
5. Confidentiality
6. Integrity
7. Accuracy
8. Timeliness
9.
10.
11. Chief Information Security Officer
12. Chief Information Officer

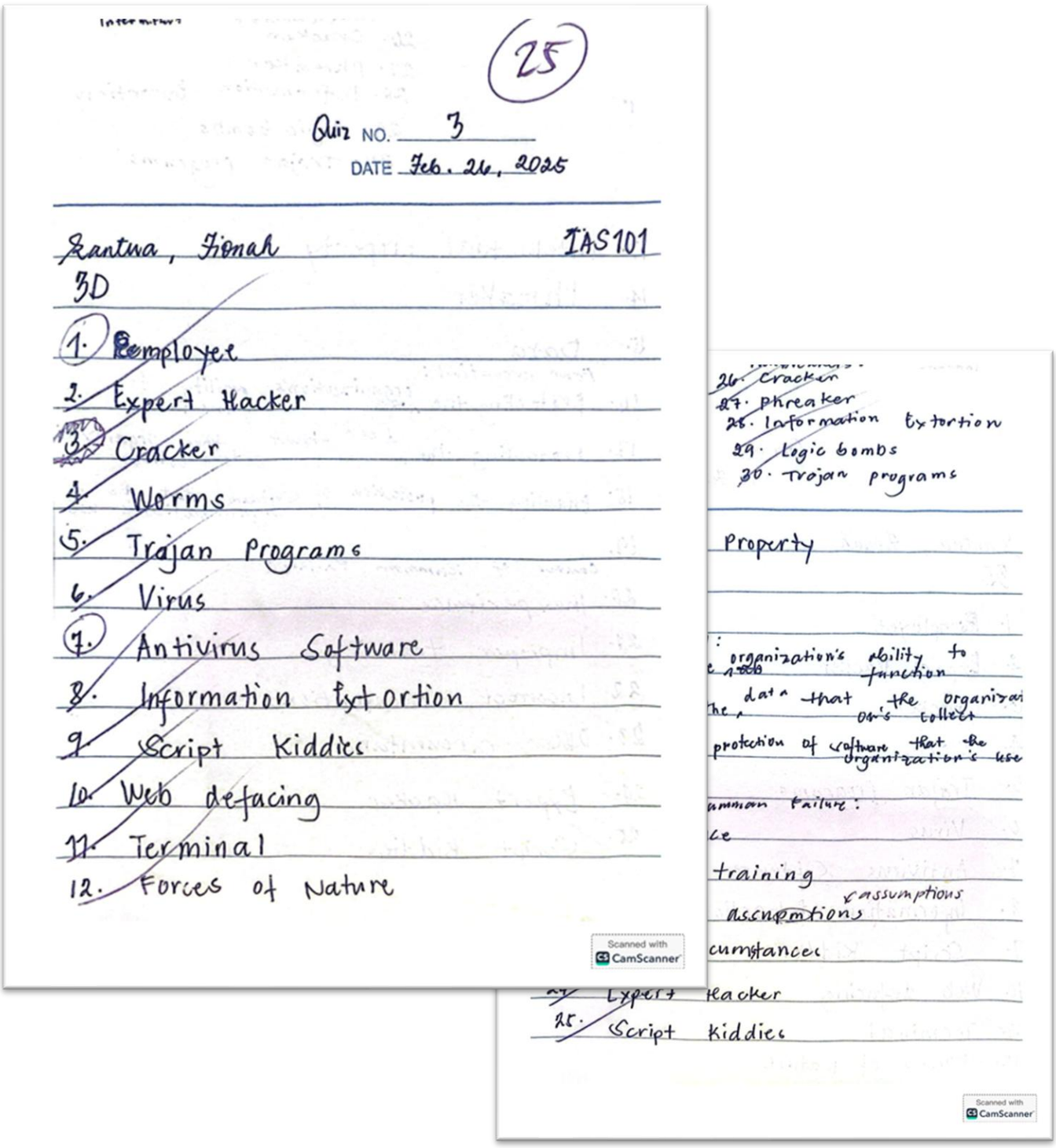
(Responsibility)
28. Data Owner
29. Data Custodian
30.

Up
Design
Design
tation
ce and Change
)
s
iality
26. Utility
27.

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 3



25

Quiz NO. 3
DATE Feb. 26, 2025

Santua, Fionah IAS101
3D

1. Employee
2. Expert Hacker
3. Cracker
4. Worms
5. Trojan Programs
6. Virus
7. Antivirus Software
8. Information tyt ortion
9. Script Kiddies
10. Web defacing
11. Terminal
12. Forces of Nature

Scanned with CamScanner

26. Cracker
27. Phreaker
28. Information tyt ortion
29. Logic bombs
30. Trojan programs

Property

organization's ability to function
data that the organizat or's collect
protection of software that the organization's use

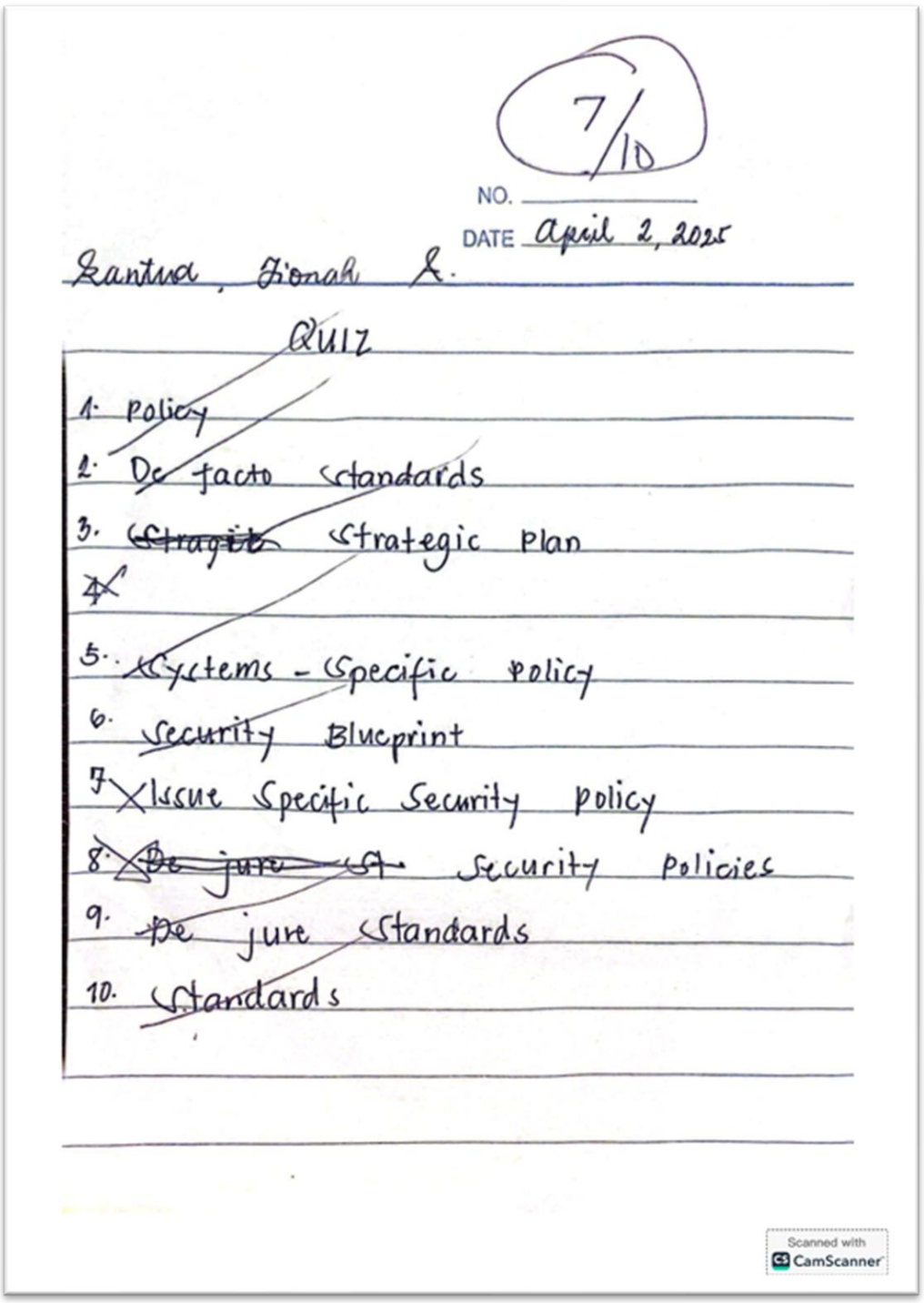
training
assumptions
Ascnomtions
cumstance

Expert Hacker
25. Script Kiddies

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 4



7/10

NO. _____

DATE April 2, 2025

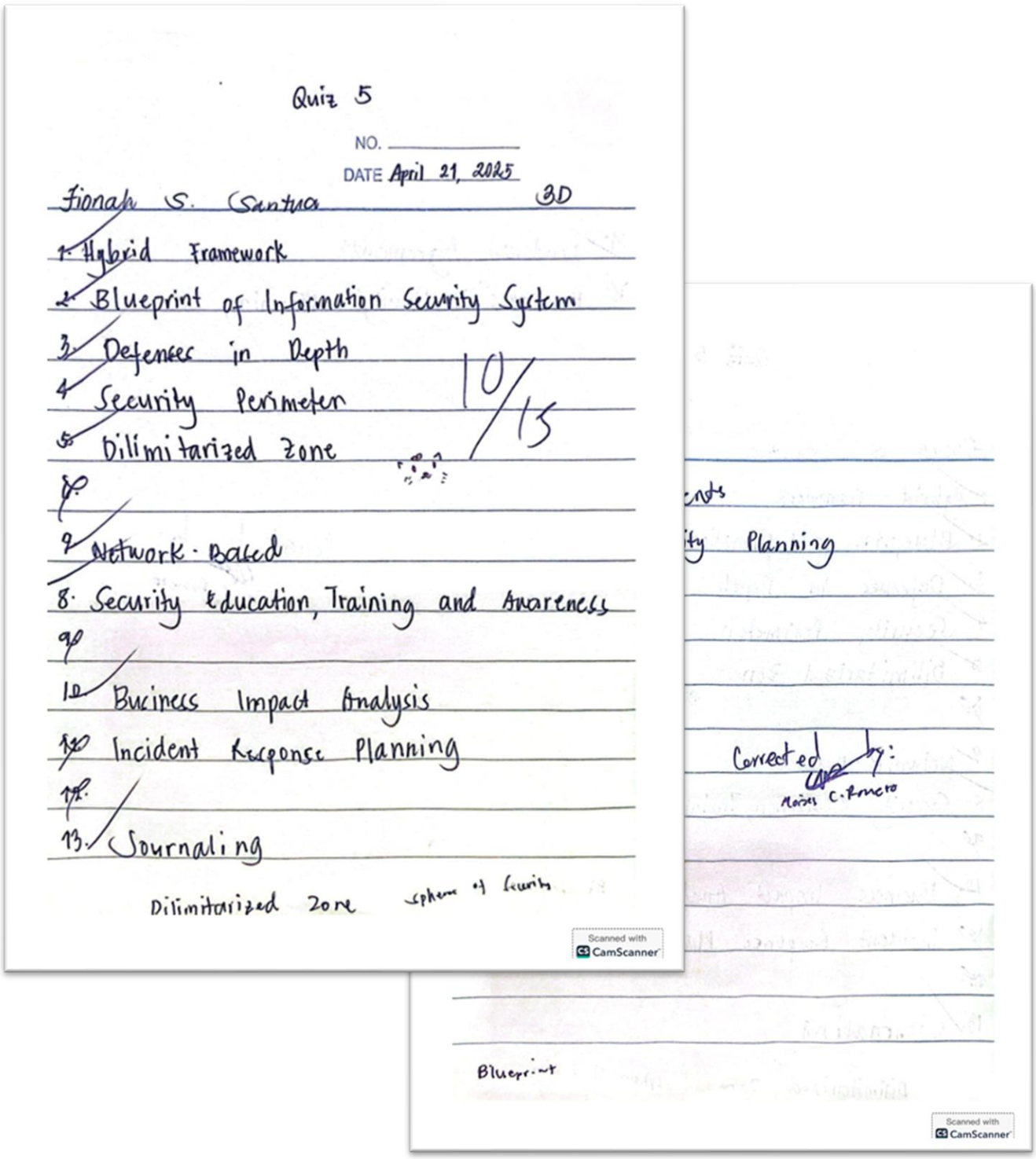
Zantua, Zionah R.

QUIZ

1. Policy
2. De facto standards
3. ~~Stragic~~ Strategic Plan
4. ~~X~~
5. Cystems - Specific Policy
6. Security Blueprint
7. ~~X~~Issue Specific Security policy
8. ~~De jure~~ ~~S~~ Security Policies
9. ~~De~~ jure Standards
10. Standards

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 5



Quiz 5

NO. _____

DATE April 21, 2025

Fionah S. Santos 3D

1. Hybrid Framework
2. Blueprint of Information Security System
3. Defenses in Depth
4. Security Perimeter 10/15
5. Dilimitarized Zone
6.
7.
8. Security Education, Training and Awareness
9.
10. Business Impact Analysis
11. Incident Response Planning
12.
13. Journaling

Dilimitarized Zone sphere of Security

Scanned with CamScanner

ents

ity Planning

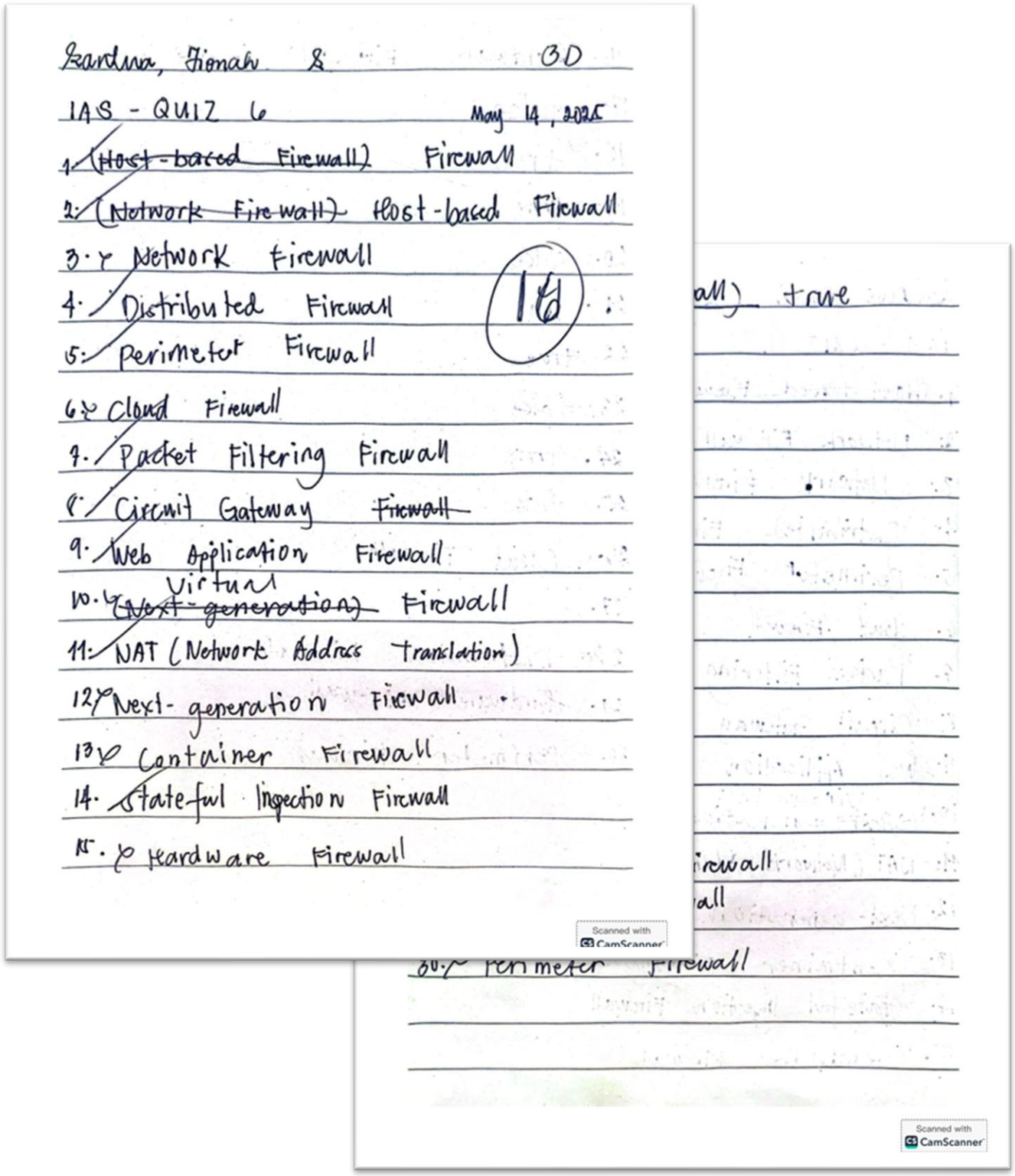
Corrected by:
Moises C. Romero

Blueprint

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

QUIZ NO. 6



Kardua, Fionah S. BD
IAS - QUIZ 6 May 14, 2025
1. ~~(Host-based Firewall)~~ Firewall
2. ~~(Network Firewall)~~ Host-based Firewall
3. Network Firewall
4. Distributed Firewall
5. Perimeter Firewall
6. Cloud Firewall
7. Packet Filtering Firewall
8. Circuit Gateway ~~Firewall~~
9. Web Application Firewall
10. ~~(Next-generation)~~ Virtual Firewall
11. NAT (Network Address Translation)
12. Next-generation Firewall
13. Container Firewall
14. Stateful Inspection Firewall
15. Hardware Firewall

16

all) true
irewall
all
30. Perimeter Firewall

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Learning Activity 3: Introduction to Information Security, Part 2

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Name: Fionah S. Santua **Year & Section:** 3D
Activity: 3 **Subject:** IAS101

Topic: Introduction to Information Security, Part 2

Twitter Celebrity Hacks (2020)

Multiple high-profile Twitter accounts were hacked in July 2020 resulting in one of the largest social media cybersecurity incidents. The hackers penetrated Twitter's internal systems through social engineering attacks aimed at employees with administrative rights. The attackers gained control of accounts that belongs to famous individuals like Elon Musk and Jeff Bezos and the former US President Barack Obama to distribute fake Bitcoin scam tweets.

- **What security characteristics failed? (*Confidentiality, Integrity, Availability)***
  - *Confidentiality* – hackers got into private accounts without permission and took control of these accounts.
  - *Integrity* – they changed the account settings (reset email addresses and passwords) to post fake tweets, misleading the users to send Bitcoin.
- **At which data state did the attack happen? *(Storage, Processing, Transmission)***
  - *Processing* – The attack happened while the system was working, they tricked the employees by pretending they were employees and got access to important tools that let them control the accounts.
- **What security controls were missing? *(Policy, Education, Technology)***
  - *Policy* – They were lacking strong policies for restricting and verifying employees access to sensitive tools that protects the accounts of the users.
  - *Education* – They were lacking knowledge about the Mandatory Multi-Factor Authentication (MFA) which indicates a lack of cybersecurity training.
- **What could have prevented the attack?**

  - A cybersecurity training could solve the problem, as it educates the employees including us to secure important information and be informed about what's the latest cybersecurity threats.

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Learning Activity 5: legal, Ethical, and Professional Issues in

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Name: Fionah S. Santua Year & Section: 3D
Activity: 5 Subject: IAS101
Topic: LEGAL, ETHICAL and PROFESSIONAL ISSUES in INFORMATION SECURITY

Read the following case scenario and answer the guided questions below.

Scenario:

A software engineer working for a tech company discovers that the company has secretly collected user data without explicit consent. The data includes browsing history, location, and personal messages. The engineer is concerned about the ethical and legal implications and considers exposing the company's actions.

Guided Questions:

1. What ethical concerns are present in this scenario?
2. Which laws (Cybercrime Prevention Act, Data Privacy Act, etc.) may be violated?
3. What role do due care and due diligence play in this situation?
4. How might jurisdiction affect the legal consequences if this happened in another country?

Answers:

1. The scenario involves ethical concerns that are aligned with the Ten Commandments of Computer Ethics: *(3) Thou shalt not use a computer to snoop around in other people's files; and (10) Thou shalt always use a computer in ways that ensure consideration and respect for other humans.* This is about **violating user privacy**; collecting data from the user without permission is wrong. The company **lacks informed consent**; users should know how their data is used, and this could lead to **unauthorized data collection** because the company is collecting data in a way that may not be legal or right. That sensitive data could be misused. Another thing is, having an **ethical choice**, the software engineer is having a dilemma and must choose whether to report this, which could affect their job.

2. The company may be held liable under these laws for secretly collecting data. The laws that could be violated are (1) **the Data Privacy Act of 2012 (RA 10173)**—this law protects personal data. Requires companies to ask permission or consent before collecting user information. It punishes those who collect, share, or throw away data without care. (2) **Cybercrime Prevention Act of 2012 (RA 10175)**—This law covers crimes like illegal access, data interference, and misuse of devices. Unauthorized data collection could be classified as illegal access or identity theft. (3) **Electronic Commerce Act of 2000 (RA 8792)**—This law recognizes legal recognition of digital records and online transactions. It punishes hacking, piracy, and unauthorized access to electronic data

3. The company failed to take due care by secretly collecting sensitive data without proper consent to inform the users. Users have the right to know their information is being collected and used, it is just basically being transparent to the users. By not doing this, the company ignored its responsibility to protect the user's privacy. The company should have implemented data protection measures in place, such as having clear privacy policies and securing data handling to comply with the privacy laws.

4. If the company operates in different countries, it could face legal consequences depending on their privacy laws. For example, in Europe, the company might be penalized under the **General Data Protection Regulation (GDPR)**, which ensures strong user data security and follows the rules. In the United States, the **California Consumer Privacy Act (CCPA)** gives users more control over their personal information, that includes allowing the users to know what data is being collect. In the Philippines, the **Data Privacy Act (RA 10173)** ensures companies handle data responsibly. Since privacy laws depend by country, the company could rreceive penalties or legal action in multiple places for collecting user data without permission.

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Learning Activity # 1 - Planning for Security

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Name: Fionah S. Santua Year & Section: 3D
Activity: 1 Subject: IAS101
Topic: Planning for Security

1. Cite at least five IT-related companies in the Philippines and identify their top cybersecurity concern.
   1. **PLDT Inc.**
      - Top Cybersecurity Concern: **Phishing Attacks**
        Cybercriminals are targeting PLDT customers with phishing scams, often using SMS (SMShing) and emails to trick users into revealing personal information or clicking malicious links.
        Source: PLDT Home doubles customer protection from cyberthreats, grants 2 years Kaspersky Premium Security to all Fiber subscribers

   2. **Globe Telecom**
      - Top Cybersecurity Concern: **Ransomware**
        Companies are moving their operations and data to the internet and the cloud, because of remote work (especially after the pandemic), employees and systems are working outside the company network. This makes it harder to protect everything.
        Source: Globe Business: Changes in Cyber Threat Exposure - Globe Newsroom

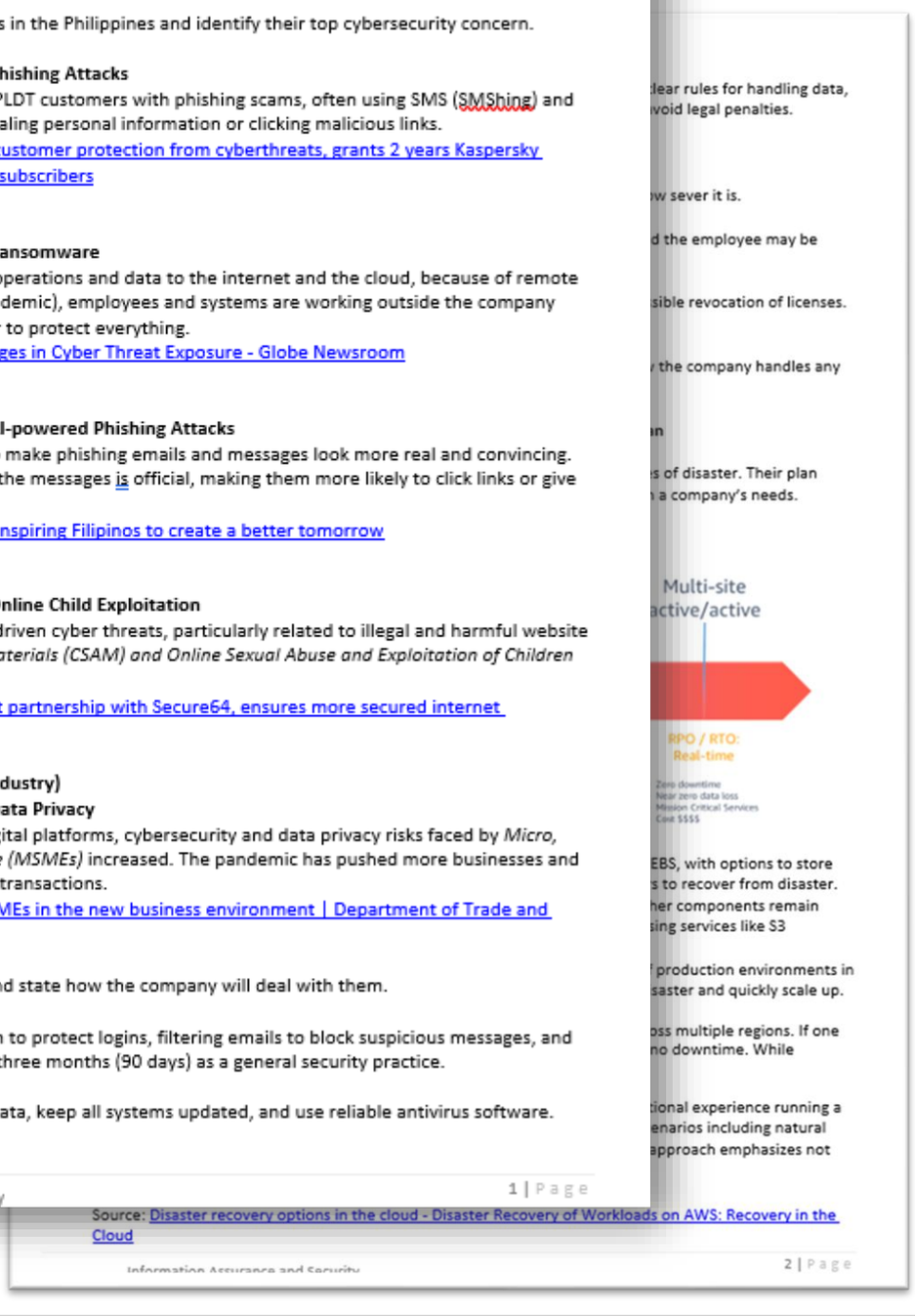
   3. **Smart Communications**
      - Top Cybersecurity Concern: **AI-powered Phishing Attacks**
        Cybercriminals are using AI to make phishing emails and messages look more real and convincing. This tricks people to thinking the messages is official, making them more likely to click links or give away personal information.
        Source: PLDT — Leading and inspiring Filipinos to create a better tomorrow

   4. **Converge ICT Solutions**
      - Top Cybersecurity Concern: **Online Child Exploitation**
        The increasing number of AI-driven cyber threats, particularly related to illegal and harmful website such as *Child Sexual Abuse Materials (CSAM) and Online Sexual Abuse and Exploitation of Children (OSAEC).*
        Source: Converge ICT rolls out partnership with Secure64, ensures more secured internet connection

   5. **DTI (Department of Trade and Industry)**
      - Top Cybersecurity Concern: **Data Privacy**
        As more business move to digital platforms, cybersecurity and data privacy risks faced by *Micro, Small, and Medium Enterprise (MSMEs)* increased. The pandemic has pushed more businesses and consumers to conduct online transactions.
        Source: Cybersecurity for MSMEs in the new business environment | Department of Trade and Industry Philippines

a) Give three cybersecurity concerns and state how the company will deal with them.
   1. **Phishing Attacks**
      - Use two-factor authentication to protect logins, filtering emails to block suspicious messages, and change your password every three months (90 days) as a general security practice.
   2. **Ransomware**
      - Regularly backup important data, keep all systems updated, and use reliable antivirus software.

Information Assurance and Security 1 | Page



STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Learning Activity # 1: Introduction to Firewall

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Name: Fionah S. Santua Year & Section: 3D
Activity: 1 Subject: IAS101
Topic: Introduction to Firewall

1. **Define what a firewall is and explain its two main functions in a network.**

   A firewall is a barrier that acts between trusted and untrusted networks. It monitors and controls the network traffic based on the security rules that are given or set up beforehand. Its two main functions are filtering the incoming and outgoing traffic to keep the network safe and preventing unauthorized access to the network by blocking suspicious traffic.

2. **Differentiate between a Packet-Filtering Firewall and a Stateful Inspection Firewall. Provide one advantage of a stateful firewall over a packet filtering firewall.**

   A packet filtering firewall works at the network layer and checks the individual data packets against the set rules. It looks things like the source of the IP, destination IP, and protocols to decide whether to allow or block the packet.

   On the other hand, a stateful inspection firewall tracks the active network connections and analyzes the context of traffic. It works at the layer 3 and 4 of the OSI model and understands the broader context of the data exchanges.

   On advantage of a stateful firewall over a packet-filtering firewall is that it examines the contents of each pocket and understands the context of the connection (data exchange), which gives a better protection because it does not just check the basic packet attributes but also looks at the state and again the context of the connection.

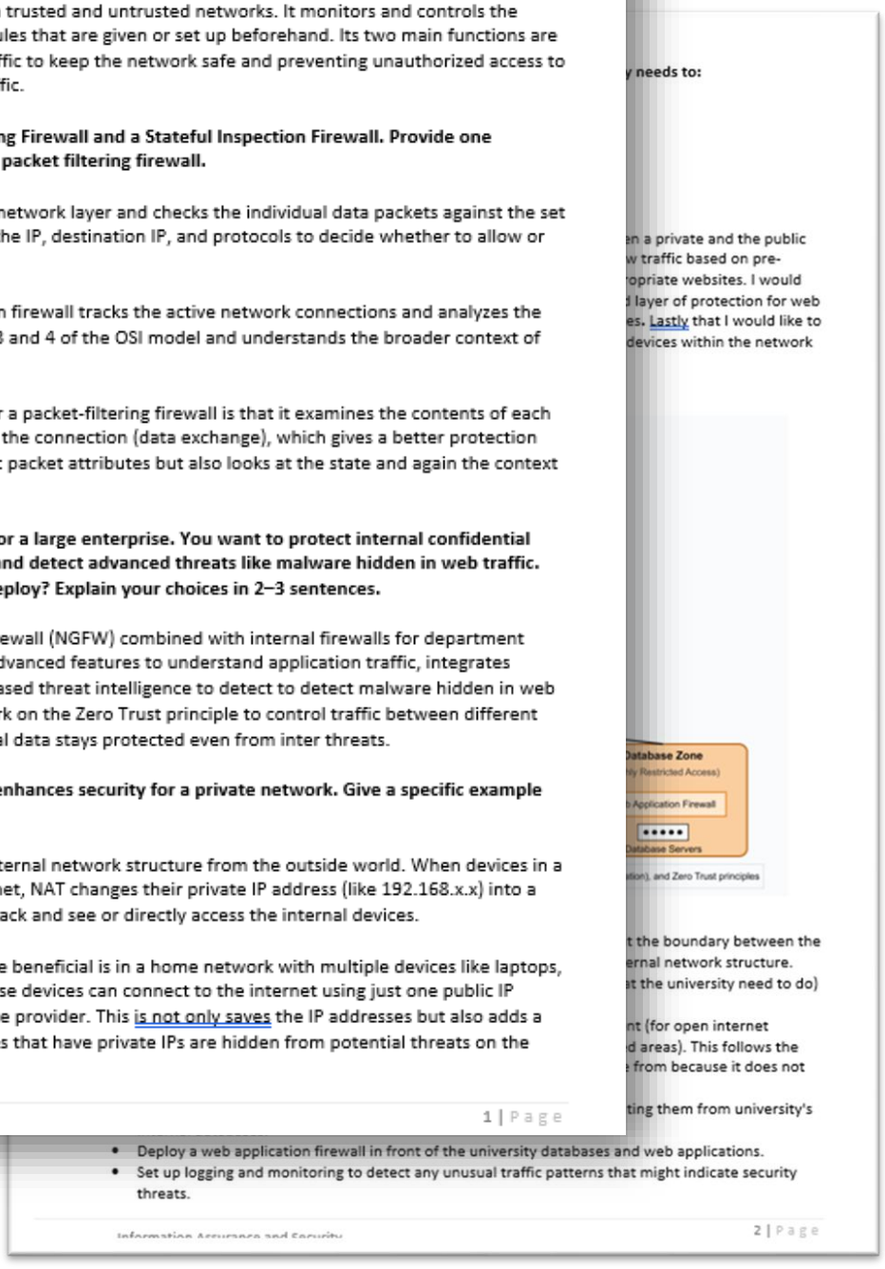
3. **Imagine you are setting up a firewall for a large enterprise. You want to protect internal confidential data, segment internal departments, and detect advanced threats like malware hidden in web traffic. Which type(s) of firewall would you deploy? Explain your choices in 2–3 sentences.**

   I would deploy the Next-Generation Firewall (NGFW) combined with internal firewalls for department segmentation. The NGRW provides a advanced features to understand application traffic, integrates intrusion prevention, and uses cloud-based threat intelligence to detect to detect malware hidden in web traffic. The internal firewalls would work on the Zero Trust principle to control traffic between different departments to ensure that confidential data stays protected even from inter threats.

4. **In your own words, explain how NAT enhances security for a private network. Give a specific example where NAT would be beneficial.**

   NAT enhances security by hiding the internal network structure from the outside world. When devices in a private network try to access the internet, NAT changes their private IP address (like 192.168.x.x) into a public IP address, making it harder to hack and see or directly access the internal devices.

   A specific example where NAT would be beneficial is in a home network with multiple devices like laptops, phones, and smart TVs. Because all these devices can connect to the internet using just one public IP address provided by the internet service provider. This is not only saves the IP addresses but also adds a layer of security since the actual devices that have private IPs are hidden from potential threats on the internet.



STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Laboratory Activity 1 - The Y2K Bug

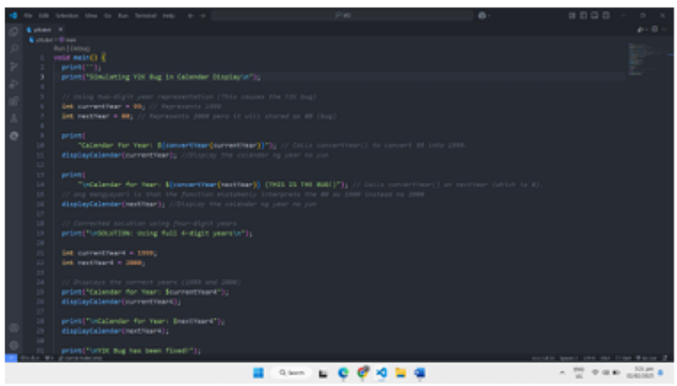
STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

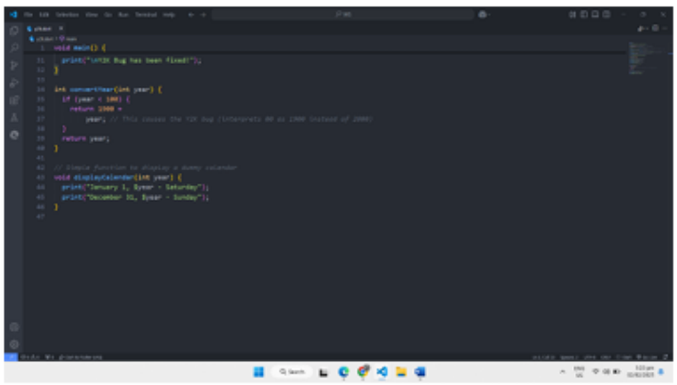
Name: Fionah S. Santua Year & Section: 3D
Activity: 1 Subject: IAS

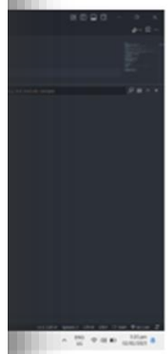
Millennium Bug

According to the National Museum of American History, 2019, the Millennium Bug, or Y2K problem, was a computer glitch that could have happened when the year changed from 1999 to 2000. Many old computer systems stored for years using only the last two digits, like "99" for 1999. The problem was that when the year turned to "00," computers might think it was 1900 instead of 2000, causing errors in calculations and system failures.

Source code written in dart:



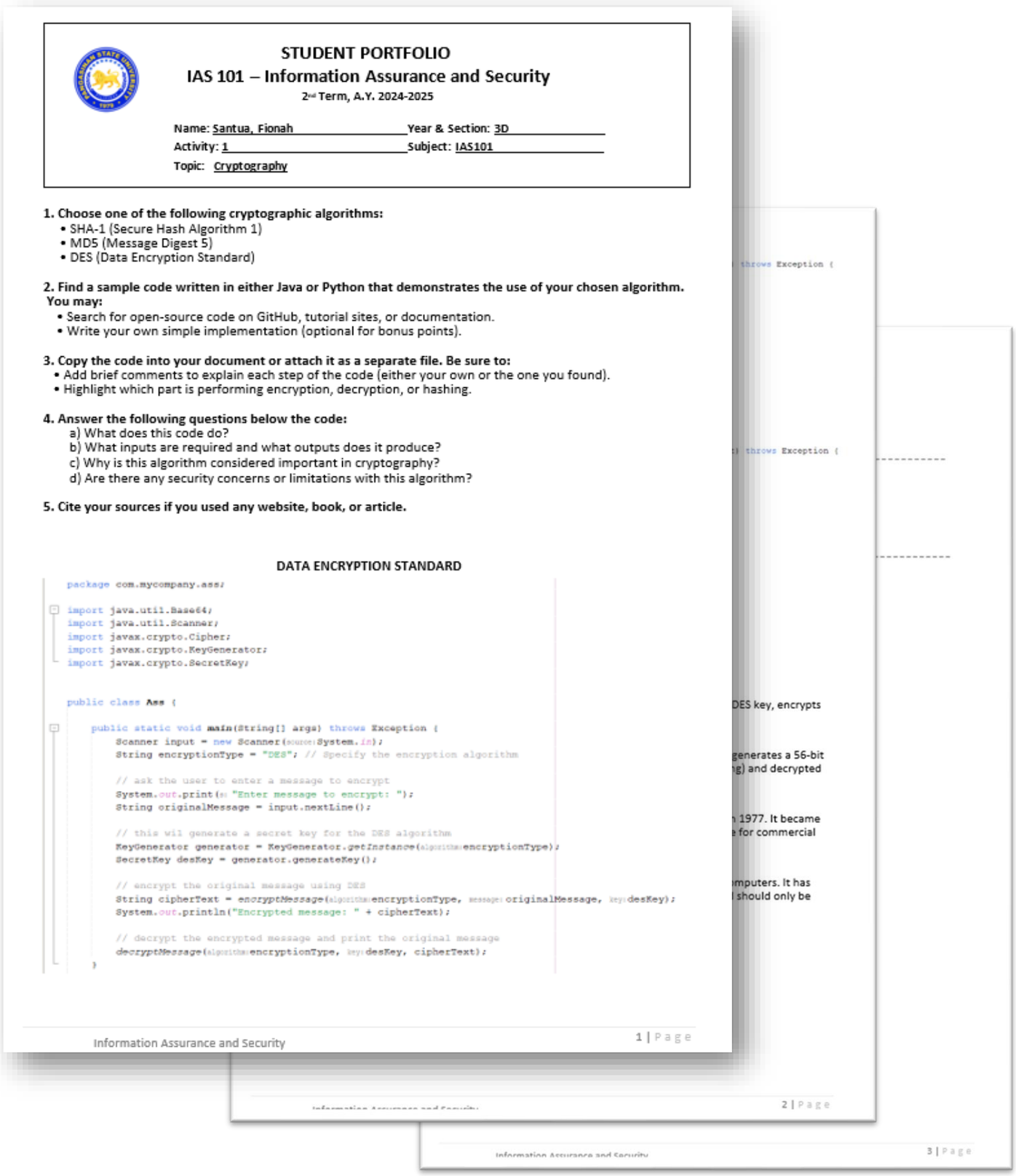




Information Assurance and Security 1 | Page

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Homework # 1 - Cryptography



STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Name: Santua, Fionah Year & Section: 3D
Activity: 1 Subject: IAS101
Topic: Cryptography

1. Choose one of the following cryptographic algorithms:
- SHA-1 (Secure Hash Algorithm 1)
- MD5 (Message Digest 5)
- DES (Data Encryption Standard)

2. Find a sample code written in either Java or Python that demonstrates the use of your chosen algorithm. You may:
- Search for open-source code on GitHub, tutorial sites, or documentation.
- Write your own simple implementation (optional for bonus points).

3. Copy the code into your document or attach it as a separate file. Be sure to:
- Add brief comments to explain each step of the code (either your own or the one you found).
- Highlight which part is performing encryption, decryption, or hashing.

4. Answer the following questions below the code:
a) What does this code do?
b) What inputs are required and what outputs does it produce?
c) Why is this algorithm considered important in cryptography?
d) Are there any security concerns or limitations with this algorithm?

5. Cite your sources if you used any website, book, or article.

DATA ENCRYPTION STANDARD

```
package com.mycompany.ass;

import java.util.Base64;
import java.util.Scanner;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;


public class Ass {

    public static void main(String[] args) throws Exception {
        Scanner input = new Scanner(source:System.in);
        String encryptionType = "DES"; // Specify the encryption algorithm

        // ask the user to enter a message to encrypt
        System.out.print(s: "Enter message to encrypt: ");
        String originalMessage = input.nextLine();

        // this wil generate a secret key for the DES algorithm
        KeyGenerator generator = KeyGenerator.getInstance(algorithm:encryptionType);
        SecretKey desKey = generator.generateKey();

        // encrypt the original message using DES
        String cipherText = encryptMessage(algorithm:encryptionType, message:originalMessage, key:desKey);
        System.out.println("Encrypted message: " + cipherText);

        // decrypt the encrypted message and print the original message
        decryptMessage(algorithm:encryptionType, key:desKey, cipherText);
    }
```

Information Assurance and Security 1 | Page

throws Exception {

throws Exception {

DES key, encrypts

generates a 56-bit
g) and decrypted

1977. It became
for commercial

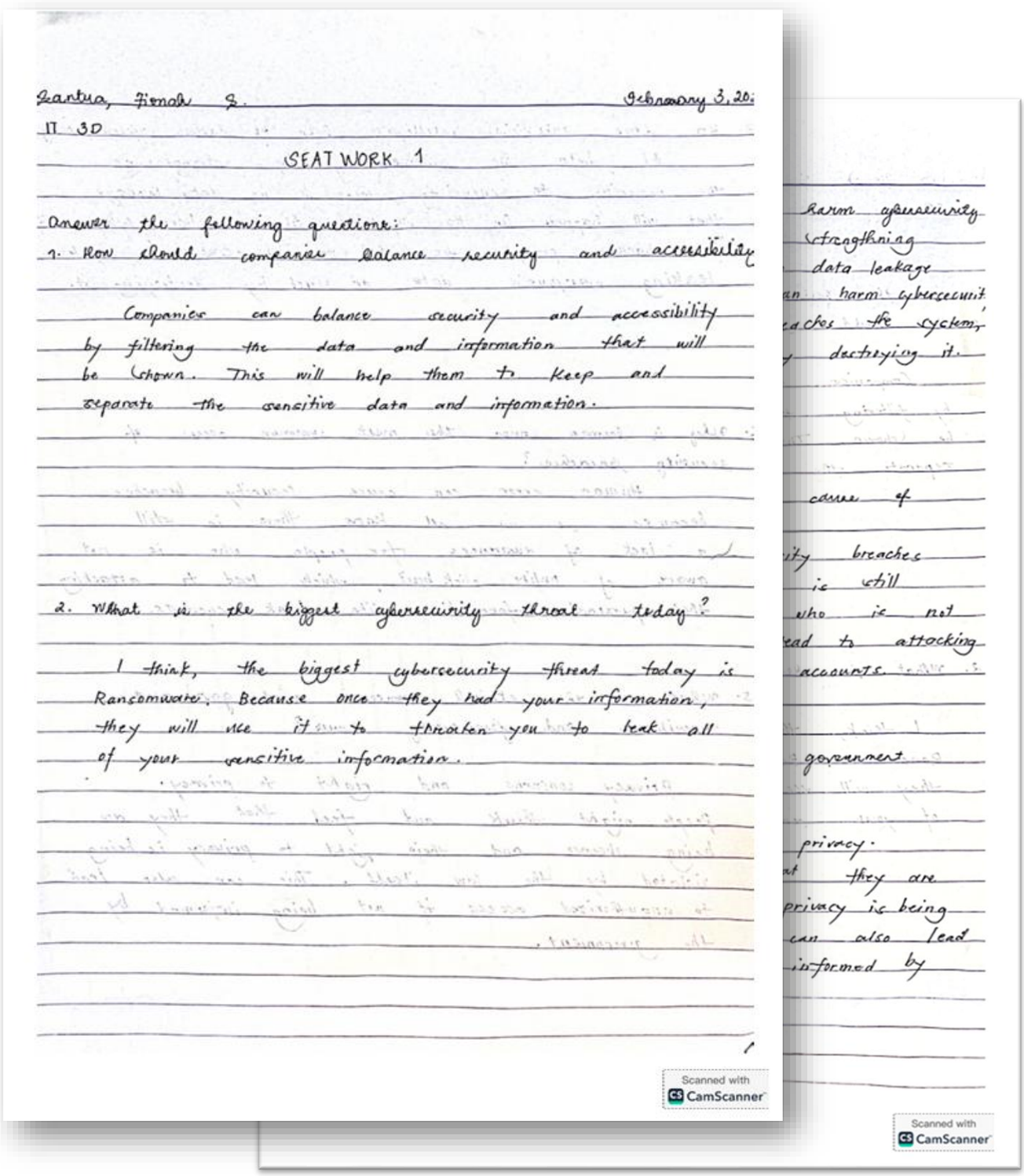
mputers. It has
should only be

Information Assurance and Security 2 | Page

Information Assurance and Security 3 | Page

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Seat Work 1: Introduction to Information Security, Part 2



Santua, Jinah S. February 3, 20
IT 3D

SEAT WORK 1

Answer the following questions:

1. How should companies balance security and accessibility

Companies can balance security and accessibility by filtering the data and information that will be shown. This will help them to keep and separate the sensitive data and information.

2. What is the biggest cybersecurity threat today?

I think, the biggest cybersecurity threat today is Ransomware. Because once they had your information, they will use it to threaten you to leak all of your sensitive information.

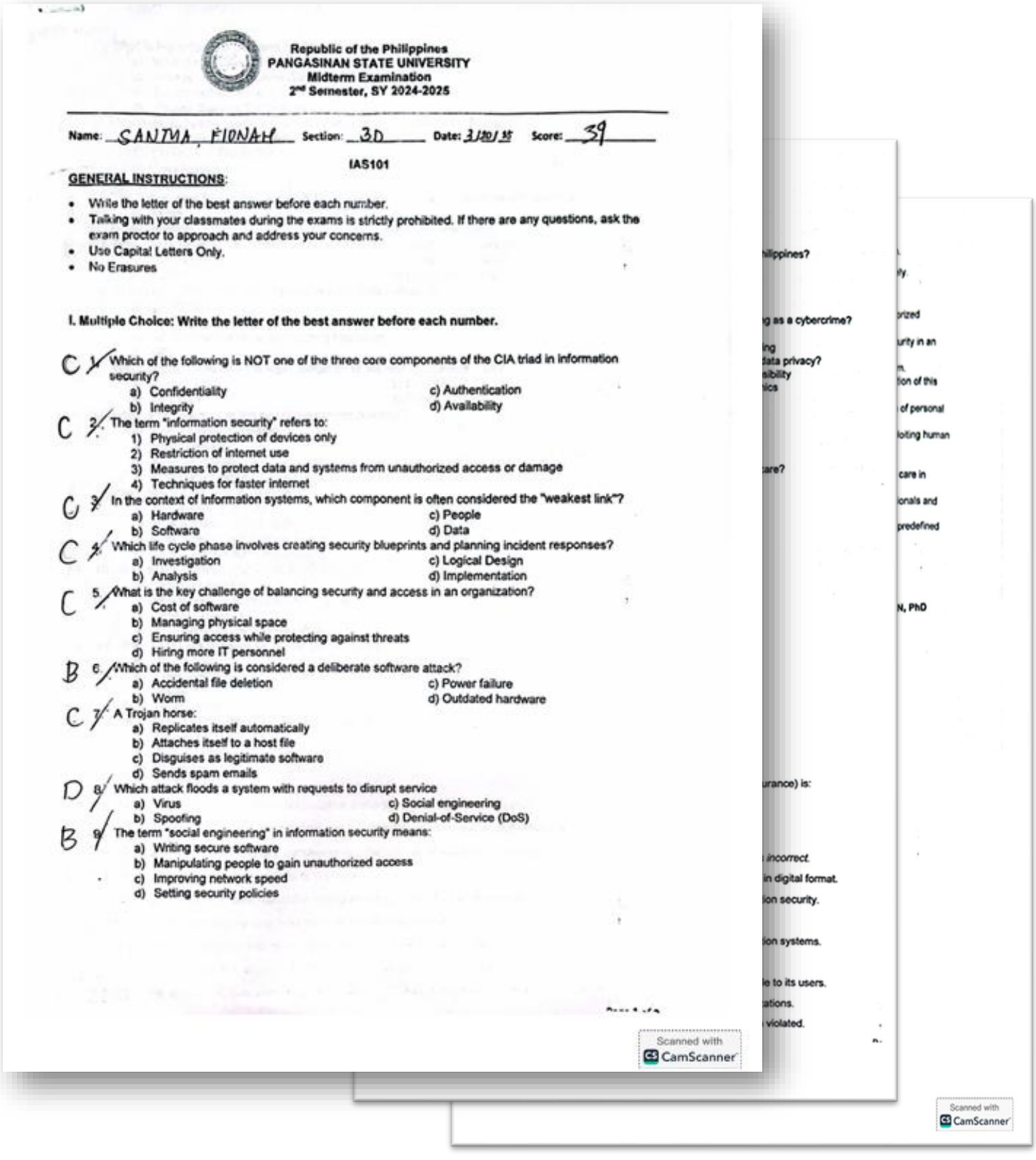
harm cybersecurity
strengthning
data leakage
an harm cybersecurit
aches the system,
destroying it.
cause of
ity breaches
is still
who is not
ead to attacking
accounts.
government
privacy.
at they are
privacy is being
can also lead
informed by

Scanned with CamScanner

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Midterm Examination



Republic of the Philippines
PANGASINAN STATE UNIVERSITY
Midterm Examination
2nd Semester, SY 2024-2025

Name: SANTUA, FIONAH Section: 3D Date: 3/20/25 Score: 39

IAS101

GENERAL INSTRUCTIONS:

- Write the letter of the best answer before each number.
- Talking with your classmates during the exams is strictly prohibited. If there are any questions, ask the exam proctor to approach and address your concerns.
- Use Capital Letters Only.
- No Erasures

I. Multiple Choice: Write the letter of the best answer before each number.

C 1. Which of the following is NOT one of the three core components of the CIA triad in information security?
a) Confidentiality c) Authentication
b) Integrity d) Availability

C 2. The term "information security" refers to:
1) Physical protection of devices only
2) Restriction of internet use
3) Measures to protect data and systems from unauthorized access or damage
4) Techniques for faster internet

C 3. In the context of information systems, which component is often considered the "weakest link"?
a) Hardware c) People
b) Software d) Data

C 4. Which life cycle phase involves creating security blueprints and planning incident responses?
a) Investigation c) Logical Design
b) Analysis d) Implementation

C 5. What is the key challenge of balancing security and access in an organization?
a) Cost of software
b) Managing physical space
c) Ensuring access while protecting against threats
d) Hiring more IT personnel

B 6. Which of the following is considered a deliberate software attack?
a) Accidental file deletion c) Power failure
b) Worm d) Outdated hardware

C 7. A Trojan horse:
a) Replicates itself automatically
b) Attaches itself to a host file
c) Disguises as legitimate software
d) Sends spam emails

D 8. Which attack floods a system with requests to disrupt service
a) Virus c) Social engineering
b) Spoofing d) Denial-of-Service (DoS)

B 9. The term "social engineering" in information security means:
a) Writing secure software
b) Manipulating people to gain unauthorized access
c) Improving network speed
d) Setting security policies

Scanned with CamScanner

STUDENT PORTFOLIO
IAS 101 – Information Assurance and Security
2nd Term, A.Y. 2024-2025

Reflection

Taking IAS 101 was initially challenging because cybersecurity concepts seemed overwhelming and technical. However, as we progressed through real-world case studies and hands-on activities, I became genuinely excited about understanding how digital threats work. The most difficult part was grasping complex encryption methods, but the activities helped make these concepts clearer. I found myself becoming more aware of security risks in my daily digital activities.

Learning Experience

This course opened my eyes to the critical importance of information security in our interconnected world. I learned fundamental concepts like risk assessment, planning for security, and the CIA triad (Confidentiality, Integrity, Availability) that form the backbone of security practices. The various attacks we studied, from social engineering to malware, showed me how vulnerable systems can be without proper safeguards. Most importantly, I gained practical knowledge about implementing security controls and developing a security-first mindset.

Conclusion

IAS 101 has fundamentally changed how I view digital security and privacy in both personal and professional contexts. The knowledge gained about threats, vulnerabilities, and protective measures will be invaluable as technology continues to evolve. This course has not only prepared me for advanced security topics but also made me a more responsible digital citizen. I now understand that information security is everyone's responsibility, not just IT professionals.