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: GODFREY F. JAVIER | 3D

PRESENTED TO: JOSHUA C. REYES

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

IAS101

26

Godfrey F. Javier — 01-02-24 3D

Quiz #1 — Introduction to Security

1.) Information Security
2.) CIA ×
3.) World War II
4.) ARPANET
5.) Ransomware
6.) RAND Report R-609
7.) Denial of Service Attack
8.) Firewalls
9.) Worm ← tanna pala
10.) Phishing and Social Engineering
11.) Accidental Vulnerabilities
12.) Multics
13.) →
13.) Y2k Problem / Millenium bug
14.) Physical Security
15.) Larry Roberts
16.) 1930s bawas! :D
17.) 1960s
18.) 1970s and 80s
19.) 1970s and 80s
20.) 1990s
21.) 1990s ×
22.) 1990s
23.) 1990s
24.) 1990s ×
25.) 1990s ×

26. False
27. False
28. True
29. True
30. False

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

QUIZ NO. 2

NO. Quiz #2

DATE _____ 3D

Godfrey F. Javier

25/30

1. Software
2. Procedure
3. McCumber Cube
4. Top-down
5. Confidentiality
6. Confidentiality
7. Timeliness
8. Availability
9. Confidentiality
10. Data
11. Chief Information Security Officer
12. Champion
13. Data Custodian

Corrected by: Kaye

Da C C End Use

28. Data Owner
29. Data Custodian
~~30. End User~~
30. Data User

~~change~~ change

Component of Info Sys

24. Data
25. People
26. Procedure
27. Network

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

QUIZ NO. 3

NO. Quiz #3

DATE

Godfrey F. Javier IAS101 3D

1. Community of Interest
2. Expert hacker
3. Cracker
4. Worm
5. Trojan Program
6. Virus
7. Antivirus Software
8. Information Extortion
9. Script kiddies
10. Web defacing
11. Terminal
12. forces of nature
13. Intellectual Property

29/30

of Service

to function

organization collec and uses

ning on organiz tion

assets IT syst m

24 Information Extortion
22. Phreaker
28 Cracker

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

QUIZ NO. 4

7/10

NO.
DATE April 2, 2025

Godfrey F. Javier

1. Policy
2. ~~De jure standard~~ De Facto standard
3. Strategic Plan
4. ~~Systems - Specific Poli~~ De jure standard
5. Systems - Specific Policy
6. Security Blueprint
7. Document Configuration Management
8. Issue Specific Security Policy
9. Security & Exchange Commission
10. Standards

corrected by:
APRIL

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

QUIZ NO. 5

11

NO. Quiz #5
DATE 04/21/25

Godfrey F. Javier

1. ~~Blueprint for Information Security System~~ Hybrid Framework
2. Blueprint for Information Security System
3. Defenses in Depth
4. Security Perimeter
5. DMZ - Demilitarized Zone
6. ~~x~~
7. Network Based
8. SETA - Security Education, Training and Awareness
9. ~~x~~
10. ~~x~~
11. ~~Disaster Recovery Plan~~ Contingency Plan
12. Shadowing
13. Journaling

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

QUIZ NO. 6

24

NO. Quiz #6
DATE 05/14/25

Godfrey F. Javier

1. Firewall
2. Host based Firewall
3. Network Firewall
4. Distributed Firewall
5. Perimeter Firewall
6. ~~Cloud Firewall~~ Virtual Firewall
7. Packet Filtering Firewall
8. Circuit Level Gateway
9. Web application Firewall
10. Managed Service Firewall
11. Network Address translation
12. Container Firewall
13. Cloud Firewall

ed Firewall
Firewall
eration Firewall
firewall
true

27. Managed Service Firewall

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: Godfrey F. Javier Year & Section: 3 D
Activity: 1 Subject: IAS

Cite at least five IT-related companies in the Philippines and identify their top cybersecurity concern.

A.) Give cybersecurity concerns and state how the company will deal with them

1.) Accenture Philippines – Phishing and Social Engineering
- Conduct regular cybersecurity awareness training for employees.
- Use AI-powered email filters to detect suspicious messages.
- Enable Multi-Factor Authentication (MFA) for all internal systems.

2.) Globe Telecom – Ransomware Attacks
- Maintain secure, encrypted, and frequent backups stored offsite.
- Use endpoint detection and response (EDR) tools.
- Isolate infected systems immediately and follow a strict incident response protocol.

3.) Trend Micro Philippines – Malware and Zero-Day Exploits
- Invest in threat intelligence and early detection sy
- Patch and update all software promptly.
- Conduct penetration testing and vulnerability ass

4.) ePLDT – Cloud Infrastructure Vulnerabilities
- Use hardened configurations and conduct cloud a
- Implement role-based access controls (RBAC).
- Use encryption for both data at rest and in transit.

5.) Pointwest Technologies Corporation – Insider Threa
- Limit access to sensitive data using the principle
- Monitor user activity with logging and alerting to
- Enforce non-disclosure agreements and conduct

B.) Cite three policy violations with the correspond

Policy Violation	Sa
Unauthorized Access to Data	1st 2nd 3rd
Sharing Login Credentials	1st 2nd 3rd
Installing Unauthorized Software	1st

IAS

striction
n

on how the company

ducts designed to protect and
hese events can range from
ors and cyberattacks. IBM's
ive events, minimizing data

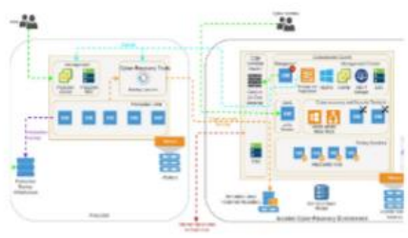
and services that aid in

at cannot be modified or

to helping you prevent and

IAS

- Cyber recovery solution
  - Isolated recovery environment solution architecture. The isolated recovery environment solution architecture uses a VMware vCenter Server® instance with the Veeam® service, gateway cluster and choices in air gap gateway options. A complete cloud solution with software licensing, virtual air gap and immutable storage, all in an easy-to-deploy automated solution.



Source: IMB Disaster Recovery Solution

- IBM's disaster recovery (DR) strategy is a comprehensive, proactive approach designed to ensure business continuity and data protection across various types of disasters, including natural events, system failures, and cyberattacks. By leveraging advanced technologies like immutable backups, AI-powered threat detection, and cloud-based recovery, IBM ensures rapid recovery with minimal downtime and data loss. Their solutions include automated failover systems, ransomware protection, and cyber resilience, enabling businesses to quickly resume operations.

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: Godfrey F. Javier Year & Section: 3D
Activity: 3 Subject: IAS

1.) What security characteristics failed? (Confidentiality, Integrity, Availability)
Confidentiality – Failed because victim's files were encrypted and held for ransom.
Integrity – Failed since the malware modified data by encrypting files, preventing legitimate access.
Availability – Failed because system files were encrypted. Many computers crashed and requires format.

2.) At which data state did the attack happen? *(Storage, Processing, Transmission)*
Storage – All files in this attack were infected and encrypted.
Processing – The systems of the victims were accessed and modified that is used to spread the malware further.
Transmission - The malware spread via the SMB (Server Message Block) protocol, affecting networked systems.

3.) What security controls were missing? *(Policy, Education, Technology)*
Policy - Organizations lacked strict patch management policies, leaving outdated systems vulnerable.
Education - Many users were unaware of cybersecurity best practices, such as not opening suspicious attachments or updating systems.
Technology - Systems were running outdated Windows versions without security patches.

4.) What could have prevented the attack?

- Based on my research, this should had been prevented if systems were updated specifically updating the OS with MS17010 security patch. Additionally, systems with heavy data can prevent their loss if they practice regular backing up of data.

1 | Page
Fundamentals of Networking 1

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: Godfrey F. Javier Year & Section: 3 D
Activity: 5 Subject: IAS

Case Study: 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 the scenario?
   - First ethical concern present in the scenario is the violation in data privacy since the company is collecting data without permission from them. Second, is the potential to harm users because personal data could lead to identity theft, financial loss, or privacy violations. Lastly, company is being dishonest to their users with their actions.

2. Which laws (Cybercrime Prevention Act, Data Privacy Act, etc.) may be violated?
   - **The Cybercrime Prevention Act of 2012:** personal messages that is accessed without consent, qualifies as illegal interception.
   - **The Electronic Commerce Act of 2000:** prohibits persons who obtain access to any electronic key, document, or information from sharing them.
   - **The Data Privacy Act of 2012:** penalizes unauthorized access or intentional breach.

3. What role do due care and due diligence play in this situation?
   - **Due Care:** Company has responsibility to ensure that the employees understand what is acceptable and unacceptable regarding data collection. Proper training and guidelines should be place in order to prevent unethical activities. Unfortunately, the company failed to implement right measures to obtain user consent and protect their information
   - **Due Diligence:** Company should have made sustained efforts to protect users' information by implementing strict security measures and obtaining user consent. But the company neglected its duty to safeguard users' rights.

4. How might jurisdiction affect the legal consequences if this happened in another country?
   - **The General Data Protection Regulation** (European Union): strict penalties for unauthorized data collection. Company would face heavy fines (€ 20 million)
   - **The Personal Information Protection Law** (China): could result in fines and business restrictions.
   - **California Consumer Privacy Act** (California): impose fines up to $7,500 per intentional violations and $2,500 per unintentional violations.

1 | Page
Fundamentals of Networking 1

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: Godfrey F. Javier 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 network security device or software that acts as a barrier between a trusted internal network and an untrusted external network. Its two main functions are to filter incoming and outgoing traffic based on predefined security rules, and to prevent unauthorized access from the network.

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 operates at the network layer and checks each data packet individually based on predefined rules. It checks the details like source and destination IP addresses, ports, and protocols to decide whether to allow or block the traffic. On the other hand, a stateful inspection firewall keeps track of active connections and it analyzes the state of the traffic over time. It works at transport and network layer and can understand the whole context of a connection, not just individual packets. One advantage of a stateful firewall is that it offers better security by monitoring the entire connection rather than just individual packets. This detects suspicious patterns and make smarter decisions about what to allow or block.

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 will deploy Next Generation Firewall along with internal firewall. NGFW allows deep inspection and malware detection hidden in web traffic. Additionally, internal firewall is good for detecting activities inside the same network, ensuring that all activities will be checked for better security against malicious intent from the employees.

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

   - Network Address Translation enhances the security of the network by hiding the internal IP address of devices instead of exposing each device's real IP. NAT translate the device IP into a single public IP when accessing the internet. One example benefit of NAT is that it keeps the internal IP address private. With that, it reduces the chance of getting attacked by hackers.

5. **You are hired as a network security consultant for a university. The university needs to:**
   • Allow students to browse the internet freely
   • Protect the university's internal databases
   • Block harmful or inappropriate websites.

Questions:
a) What firewall configurations and placements would you recommend?

Information

1 | Page

al Firewall to strengthen
work perimeter to inspect
vall will monitor and
niversity's internal
ll to block harmful or

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: Godfrey F. Javier Year & Section: 3 D
Activity: 1 Subject: IAS

Millennium Bug

A computer flaw, the so-called "Millennium Bug," led to anxiety and the Y2K (Year 2000) scare. When complex computer programs were first written in the 1960s, engineers used a two-digit code for the year, leaving out the "19." As the year 2000 approached, many believed that the systems would not interpret the "00" correctly, therefore causing a major glitch in the system. (NatGeo)

Sample Scenario:

```
Imagine the date today is December 30, 1999. After 2 days, the year will be 2000
Current Year: 1999 (Converted to 4 digits)
Year after 2 days: 1900 (Converted to 4 digits) (THIS IS THE BUG)

The problem is that data that was derived from the date will probably give error.

Person's year of birth is 40 (1940)
This is the age of person in current year: 59
This will be the age of the person next year: -40 (Wrong)
```

Why did this happen?

- Based on my research, computer engineers back then used only the ones and tens digits of the year because data storage in computers was costly and took up a lot of space.

My solution

- The possible solution for this is to update all systems, allowing the computer's year to handle four-digit numbers and always foresee potential problems in the future.

```
SOLUTION: Updating dates of the system making the year 4 digits.
Person's year of birth is 1940
This is the age of person in current year: 59
This will be the age of the person next year: 60
Y2K Bug SOLVED!
```

Source code written in dart:

1 | Page

Fundamentals of Networking 1

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: Javier, Godfrey **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 (Implemented by Godfrey)

```
public class Ias {

    public static void main(String[] args)  throws Exception{
        Scanner s = new Scanner(System.in);
        //key must be DES in order to use the DES Algorithm
        String key = "DES";

        System.out.print("Enter a word to encrypt: ");
        String word = s.nextLine();
        // Generate a DES key
        KeyGenerator keyGen = KeyGenerator.getInstance("DES");
        SecretKey secretKey = keyGen.generateKey();

        System.out.println("The encrypted word is: "+enc(key,word,secretKey));

        dec(key, word, secretKey);
    }

    //Returns the encrypted word using DES
    public static String enc(String key, String word, SecretKey secretKey)throws Exception{

        // Create Cipher instance and initialize for encryption
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);

        // Encrypt the text
        byte[] encryptedBytes = cipher.doFinal(word.getBytes());
        String encryptedText = Base64.getEncoder().encodeToString(encryptedBytes);

        return encryptedText;

    }


    //Prints the decrypted text
    public static void dec(String key, String word,  SecretKey secretKey, String encryptedText) throws Exception{
        // Initialize the cipher for decryption
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.DECRYPT_MODE, secretKey);

        // Decrypt the text
        byte[] decryptedBytes = cipher.doFinal(Base64.getDecoder().decode(encryptedText));
        String decryptedText = new String(decryptedBytes);
        System.out.println("Decrypted text: " + decryptedText);
    }
}
```

Information Assurance and Security 1 | Page

r using Data Encryption Standard.

t produce?
key must be "DES" in order to use the DES

tography?
ely accepted and used by the U.S. government
77 as a federal standard.

this algorithm?
2 quadrillion possible keys in DES, modern
reason is that DES is not good for encrypting

tGPT.

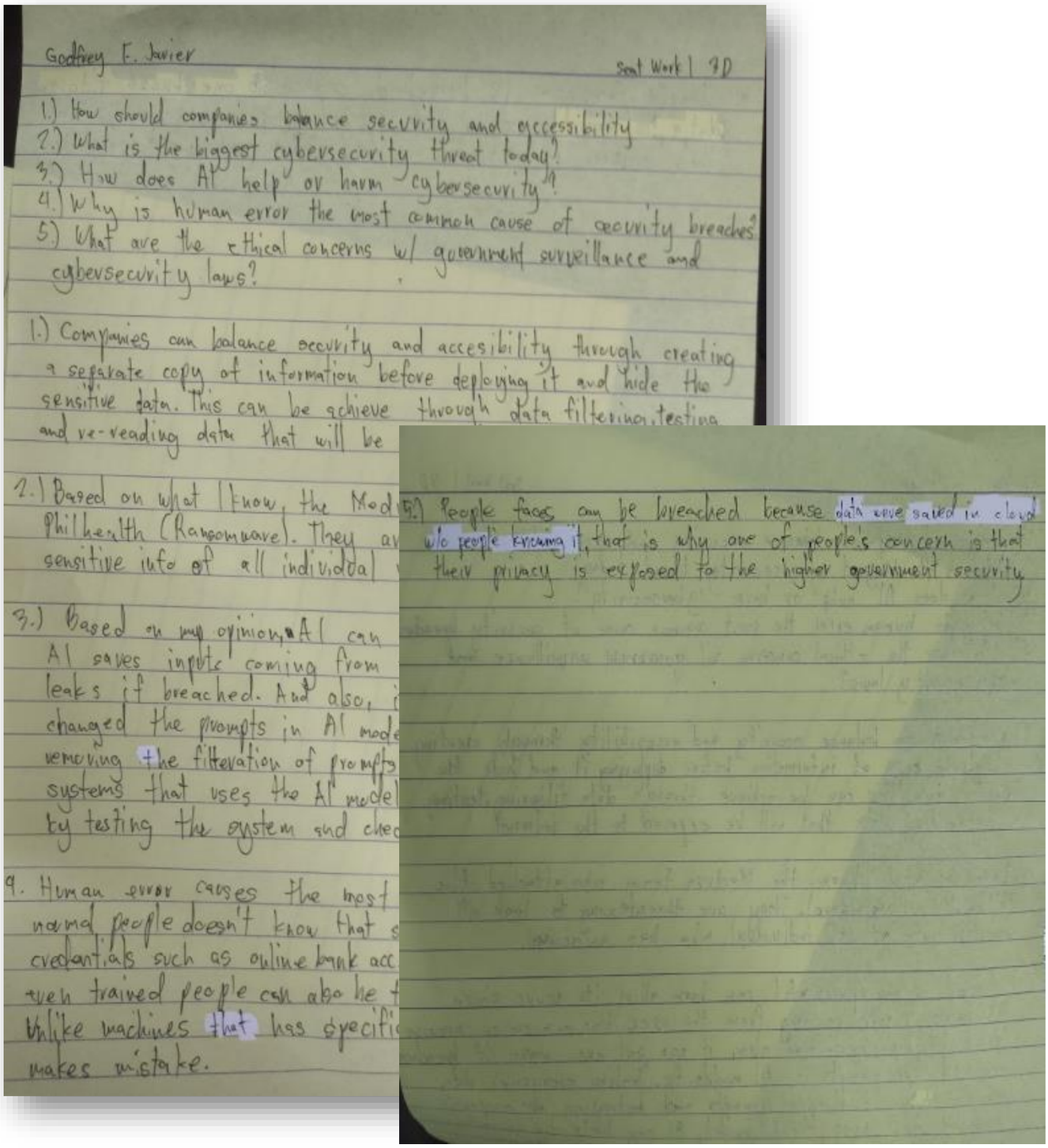
me text input

S DES algo
Xi1Z2k3mOfyr5dFPsNit7FpWI=
o

AS DES algo
DCjju8jJNPbbQmmjYKpNYDazYk=
go

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

Seat Work 1: Introduction to Information Security, Part 2



Godfrey E. Javier

Seat Work 1 3D

1.) How should companies balance security and accessibility
2.) What is the biggest cybersecurity threat today?
3.) How does AI help or harm cybersecurity?
4.) Why is human error the most common cause of security breaches?
5.) What are the ethical concerns w/ government surveillance and cybersecurity laws?

1.) Companies can balance security and accesibility through creating a separate copy of information before deploying it and hide the sensitive data. This can be achieve through data filtering, testing and re-reading data that will be

2.) Based on what I know, the Mod
PhilHealth (Ransomware). They ar
sensitive info of all individual

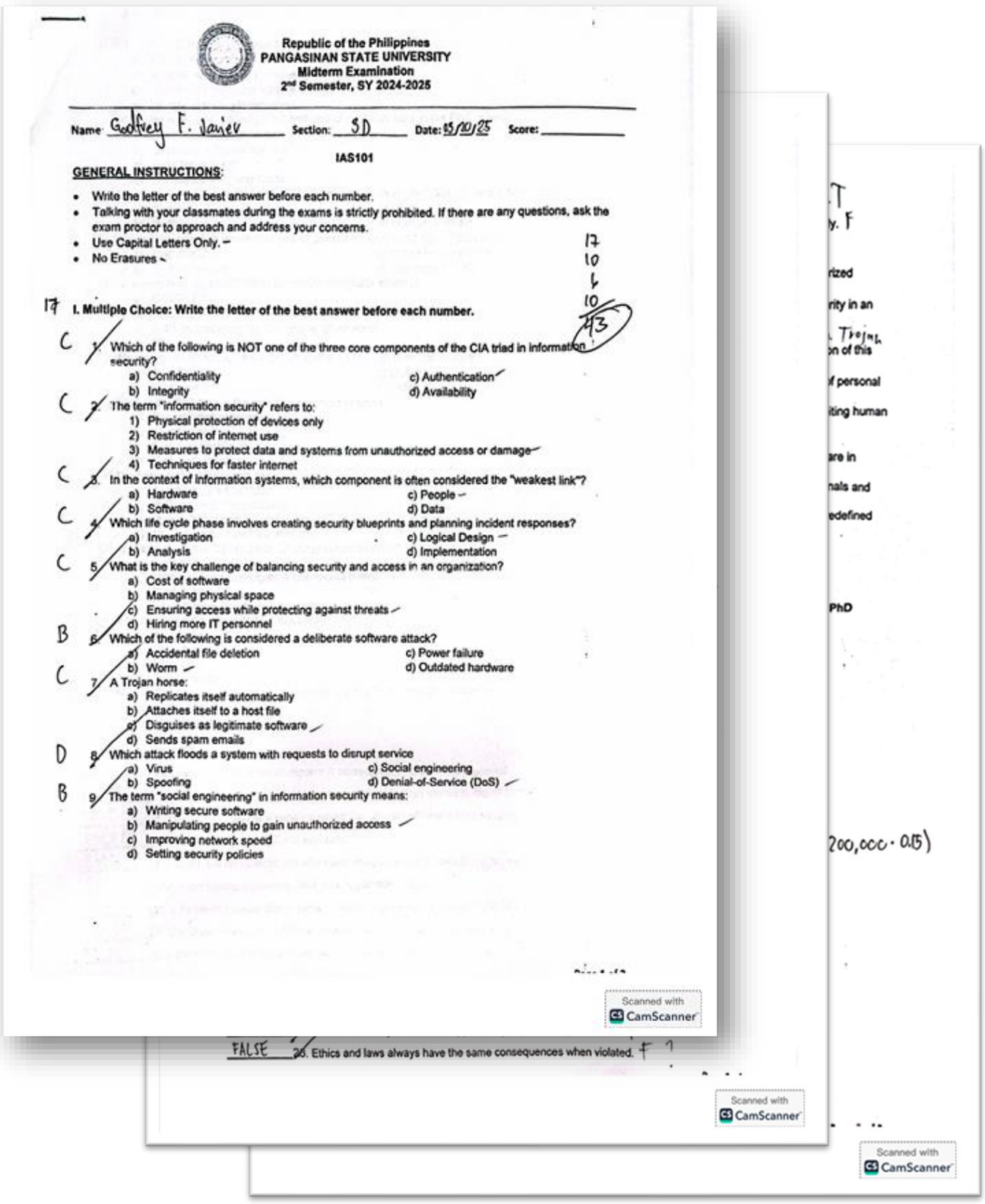
3.) Based on my opinion, AI can
AI saves inputs coming from
leaks if breached. And also,
changed the prompts in AI mode
removing the filteration of prompts
systems that uses the AI model
by testing the system and chec

4. Human error causes the most
normal people doesn't know that
credentials such as online bank acc
even trained people can also be
Unlike machines that has specific
makes mistake.

5.) People faces can be breached because data are saved in cloud
w/o people knowing it, that is why one of people's concern is that
their privacy is exposed to the higher government security

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: Godfrey F. Javier Section: 5D Date: 05/20/25 Score: _____

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.

17
10
6
10
43

17 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
b) Integrity
c) Authentication
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
b) Software
c) People
d) Data

C 4. Which life cycle phase involves creating security blueprints and planning incident responses?
a) Investigation
b) Analysis
c) Logical Design
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
b) Worm
c) Power failure
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
b) Spoofing
c) Social engineering
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

FALSE 26. Ethics and laws always have the same consequences when violated.

Scanned with CamScanner

Scanned with CamScanner

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

Reflection

This course was both eye-opening and exciting. It introduced me to the deeper world of cybersecurity and made me realize just how important online safety is. I became genuinely curious especially about hacking and found it fascinating how complex and impressive it can be. But sometimes, the course is challenging because of weekly quizzes, the quizzes are hard and challenging especially of new terminologies I encountered.

Learning Experience

Throughout the course, I learned a lot about how cybersecurity works in real-world settings. I now understand the different layers of security that companies use to protect their systems, and the role of firewalls, how they work and the types that exist. I also found the history of cybersecurity really interesting, seeing how it has evolved over time. Concepts like NAT and the various threats to data safety gave me a clearer picture of the challenges in keeping information secure. Overall, the course gave me a solid foundation and a better appreciation of how critical cybersecurity is today.

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

Conclusion

This course helped me learn a lot about cybersecurity and made me really interested in the topic. Even though some parts were difficult, like the quizzes and new terms, I still gained useful knowledge. Most importantly, I now understand how important it is to protect ourselves online and that cybersecurity is something everyone should know about, not just experts