**Hardware Vulnerability Research**

**CYBR3020**

**Vulnerabilities and Exploits**

Arr Domingo

Student ID: 200458099

Instructor: Clayton Amelia

Table of Contents

[Introduction 1](#_Toc210408021)

[Topic 1 1](#_Toc210408022)

[Subtopic 1.1 1](#_Toc210408023)

[Subtopic 1.2 1](#_Toc210408024)

[Subtopic 1.3 2](#_Toc210408025)

[Topic 2 2](#_Toc210408026)

[Subtopic 2.1 2](#_Toc210408027)

[Subtopic 2.2 2](#_Toc210408028)

[Subtopic 2.3 2](#_Toc210408029)

[Subtopic 2.4 2](#_Toc210408030)

[Topic 3 2](#_Toc210408031)

[Subtopic 3.1 2](#_Toc210408032)

[Subtopic 3.2 2](#_Toc210408033)

[Subtopic 3.3 2](#_Toc210408034)

# Introduction

In today’s digital age, organizations are exposed to an intentional and unauthorized actions against a computer system or network to compromise its data or functionality. Such action includes cyberattack, cyber intrusion, security breach, malicious hacking, and unauthorized access.

# How the Exploit Works

One of the crucial components of an organization’s security strategy is often referred to as Identity and Access Management (IAM). IAM ensures that the right people, machines, and software components access the right digital resources at the right time and for the right reasons.

## Subtopic 1.1

IAAA (Identification, Authentication, Authorization, Accountability) is the foundation of Identity and Access Management (IAM). IAM is a discipline and a type of framework for solving the challenge of secure access to digital resources.

# What was/is vulnerable?

## Subtopic 2.1

## Subtopic 2.2

# How to Prevent the Exploitation

## Subtopic 3.1

## Subtopic 3.2

References