# Fullstack Academy

# Penetration Testing Report
## Career Simulation 3

Created by: Ivan Arias

Engagement Contacts:

- Ozzy Pratt
- Robert Cain
- Rachel Scott
- Soraya Rampersad

# Executive Summary

: This section provides a high-level summary of what was found during the engagement. High-level executives should be able to understand what happened by reading this summary—without needing a deep knowledge of the TTPs involved in the engagement.

Objective

[Replace this text with the objective of the penetration test. This should restate the penetration test's purpose, direction, and scope.]

Tools Used

[Replace this text with the tools you used during the penetration test. Provide a brief description of the tools for a non-technical audience.]

Introduction

# Penetration Test Findings

## Summary

[Update the table below with your findings (i.e. insecure files, weak passwords, etc) and severity levels (high, medium, or low).]

| Finding # | Severity | Finding Name |
|---|---|---|
| HTTP (1013/tcp) | High | Apache http 2.4.52 on Ubuntu |
| SSH (2222/tcp) | Severity | OpenSSH 8.9p1 on Ubuntu |
| | Severity | |
| | Medium | |
| | Severity | |

## Detailed Walkthrough

[Replace this text with a walkthrough of how you discovered your findings. Include screenshots, graphics, etc. as evidence.]

Attack Path: For the technical staff, this section meticulously details the path that could be taken to compromise a high-value target, such as a DC or a sensitive server. It serves as a reminder of the potential vulnerabilities and the need for robust security measures.

Vulnerability and Exploitation Details: This section shows all the vulnerabilities found during testing. This section shows how exploitable vulnerabilities were exploited and might include descriptions or pictures. This is usually just a list of the vulnerabilities found from a vulnerability scan.

Impact: Some vulnerabilities might have a greater impact than others. For exploited vulnerabilities with a high impact, like remote code execution, this section shows how detrimental exploiting a vulnerability can be.

Tools Used: This section shows the tools used during the engagement.

Summary