**Happy Accident Labs Penetration Testing**

Nwachukwu Edumanichukwu

Bellevue University

CYBR 430, Penetration Testing and Incident Response

Professor Kyle Kennedy

March 16, 2023

Cover Page:

• Title: Black-box Penetration Test Report for Happy Accident Labs

• Date: March 16, 2023

• Prepared by: Nwachukwu Edumanichukwu

• Project Sponsor: Bill Winnicott, CIO

Index (to be added to as the report grows):

• Executive Summary

• Objectives

• Scope

• Authorization

• Assumptions

• Legal Restrictions

• Methodology

• Vulnerabilities and Recommendations

• Conclusion

Executive Summary:

The executive summary should provide a brief overview of the report, highlighting the key findings and recommendations. Here are some sub-sections that should be included:

• Project Objectives: The primary objective of the black-box penetration test is to identify any vulnerabilities in Happy Accident Labs network that could be exploited by unauthorized individuals to gain access to confidential information or compromise the integrity of the system. This will help the company to better protect its intellectual property and prevent any potential security breaches.

• Scope of the Project: The scope of the project covers the entire organizational network of Happy Accident Labs, including all company-owned assets. However, it does not include the networks of any clients or suppliers, and any outsourced services can be viewed but not hacked. The test should not impact the operation of any system, and the teams cannot stop work while the test is being conducted.

• Authorization: The penetration test has been authorized by the company's management, and all legal requirements have been met.

• Assumptions: The assumptions made in conducting the test includes the use of standard tools and techniques, the absence of any insider threats or malicious intent, and the assumption that the network is adequately secured.

Legal Restrictions:

Before conducting the penetration test, we will research the local, state, and federal laws that are in place governing penetration testing activities for Happy Accident Labs. We will also ensure that all legal requirements are met before starting the test.

Methodology:

The black-box penetration test was conducted using a combination of manual and automated testing techniques. The testing team used both open-source and commercial tools to identify vulnerabilities in the network. The team followed a defined methodology that included the following steps:

Information Gathering

Vulnerability Scanning

Manual Testing

Exploitation and Privilege Escalation

Reporting

Vulnerabilities:

The findings of the black-box penetration test revealed several vulnerabilities in Happy Accident Labs' IT infrastructure. These vulnerabilities included:

Weak Passwords

Outdated and Unpatched Software

Unsecured Network Devices

Lack of Encryption

Poor Access Controls

Recommendations:

Based on the findings of the penetration test, we recommend the following actions to improve the security of Happy Accident Labs IT infrastructure:

Implement Strong Password Policies

Keep Software and Systems Up-to-Date and Patched

Secure Network Devices with Strong Passwords and Encryption

Use Encryption to Protect Sensitive Data