**Happy Accident Labs Penetration Testing Report**

Nwachukwu Edumanichukwu

Bellevue University

CYBR 430, Penetration Testing and Incident Response

Professor Kyle Kennedy

May 14, 2023

Executive Summary

Objectives: The primary objective of this penetration test project is to identify any vulnerabilities inside Happy Accident Labs network. This penetration test project will also assess the organization's data security by identifying potential vulnerabilities and the extent to which they could compromise confidentiality, integrity, and availability.

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 would not impact the operation of any system.

Project Objectives: The primary objective of the black-box penetration test is to identify any known 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.

Authorization: This penetration test has been authorized by HAL’s CIO Bill Winnicott. We have been authorized to access HAL’s networks, systems and conduct these tests according to the agreed terms and while staying within all legal requirements.

**Summary of Findings**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Vulnerability Name | Affected Host | Impact | Risk Likelihood |
| 1 | Domain | Happyaccidentlabs.com | Data Leak | Low |
| 2 | MS17-10 – Eternal Blue | 10.19.99.105 | Compromised access to system | High |
| 3 | Weak Password Policy | All the hosts | Unauthorized access to systems and data | High |
| 4 | Unsecured SMB Shares | HAL\_FS  HAL-PC-001  HAL-PC-005 | Unauthorized access to systems and data | High |
| 5 | Weak firewall configuration | 10.19.99.105 | Increased risk of unauthorized access | High |
| 6 | Weak Wi-Fi Security | HAL\_WiFi | Unauthorized access to network | High |
| 7 | Backdoor access | 10.19.99.105 | Unauthorized access to systems and data | High |
| 8 | Poorly secured and unrestricted file shares | HAL-PC-001  HAL-PC-003  HAL-PC-004 | Unauthorized access to data | High |

Details of vulnerabilities:

1. **Weak password policy:** This is when passwords of devices, accounts and networks are not complex enough to secure data. The Network/IT Admin should implement stronger password policies. The password polices was not complex enough and this made it easier to crack the hashed password faster and easier.
2. **MS10-17 Eternal Blue:** This is an exploit developed by the U.S National Security Agency (NSA). This was leaked by a hacker group named shadow broker. This exploit takes advantage of the vulnerability in SMBv1 protocol on windows OS. Microsoft released a patch for this vulnerability, but HAL systems are not up to date.
3. **Unsecured SMB Shares:** This is when the SMB shares do not have a proper security measure in place.
4. **Backdoor access:** This is an unauthorized entry access created by attacks to gain unauthorized access to networks and systems without authentication.
5. **Weak firewall access:** This occurs when the firewall of a company’s network security system designed to protect a computer or network from unauthorized access is not configured properly to achieve the intended level of security.
6. **Weak Wi-Fi Security:** This is the inability to safeguard the privacy and integrity of data transmitted over the organization’s network due to weak or outdated encryption protocols.

**Proof of Concept**

***Exposure of passwords:***

Text

Description automatically generatedThe hashed password was easily cracked revealing a weak password that did not have an adequate password policy implemented.

***Unsecure SMB Shares:***

Text

Description automatically generatedThe cracked passwords was used to gain access to the shared drives.

**Graphical user interface, text

Description automatically generated**

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

***Backdoor Access:***

**Text

Description automatically generated**

**Text

Description automatically generated**

***MS10-17 EthernalBlue:***

Text

Description automatically generated