A black text on a white background

Description automatically generated

[Company Name]

**Security Assessment Report**

Performed by [Team Name]

[Date]

This report contains confidential and sensitive information. It is intended solely for the information and use of *[Company Name]*

A black text on a white background

Description automatically generated

This engagement was performed in accordance with the signed agreements put forth by *[Company Name]*, and the procedures were limited to those described in the scope and rules. The findings and recommendations resulting from the assessment are provided in this report. Given the time-limited scope of this assessment, the findings in this report should not be taken as a comprehensive listing of all security vulnerabilities.

|  |  |
| --- | --- |
|  | Executive Summary |

## 

|  |  |
| --- | --- |
| *[Company Name]* requested a comprehensive penetration test against [FIXME: add scope/which features are being tested]. This assessment was executed in two stages: the pre-engagement operations consisting of open-source intelligence gathering, and the assessment phase consisting of active reconnaissance and leveraging exploits to prove the existence of system vulnerabilities. The following report outlines the findings from these engagement phases as well as mitigations for pressing issues.  [FIXME: Here we should talk about how critical systems are in place and were carefully tested, also bring up specific data laws pertinent to the specific company type]. Subsequently, you will find a high-level summary and strategic suggestions from *[Team Name]* below. High-Level Summary/Compliance*[Team Name]* noticed [N] vulnerabilities all related to [whatever]. [Team name] found that [Company name] followed compliance (state specific orders) well with [whatever]. However, testing showed that the company lacked compliance when it came to [whatever] Strategic Recommendations To improve the security posture of *[Company Name]*, *[Team Name]* recommends pursuing the following strategies:  **Immediate Actions**   * [FIXME: add findings]   **Long-Term Strategies**   * [FIXME: add findings] | **Timeline**  Engagement  Began  *[Date Begin]*  Engagement  Concluded  *[Date end]* |
| **Findings**  **N** Critical  **N** High  **N** Medium  **N** Low  **N** Informational |

## Scope

*[Team Name]* performed security testing on *[Company Name]* network infrastructure. Testing was conducted from the perspective of an attacker with a connection to the external network of *[Company Name]*. *[Team Name]* was provided the following networks to test from the scope of work created by *[Company Name]*.

[INSERT TABLE]

Special care was taken to exclude the following specified networks/hosts.

[INSERT TABLE]

|  |  |
| --- | --- |
|  | Technical Findings |

[INSERT TABLE OF CONTENTS]

## 

## *Critical Severity Findings*

|  |  |
| --- | --- |
| Name | **01** |

#### Security Implications

[Short 1-2 sentence paragraph about the high-level impact to the organization and how it is generally performed. (e.g., An unauthenticated attacker can leverage an intentional backdoor in VSFTPD version 2.3.4 to gain an authenticated session as the root user on a machine)]

#### Description

[Talk about how you found it! Show screenshots and proof to the point where they could follow along and achieve the same outcome as you. Explain a bit more and maybe give some important context that is needed.]

#### Affected Systems

[List of hostnames and/or ips that are affected]

#### Recommendations

[Give a paragraph or list of recommendations. Keep it a bit higher-level but if some short commands are all that is necessary you can put them here too]

#### References

[Give any references used here. This includes something like exploitDB or a microsoft advisory posting. If linking github, make sure it is a static page that won’t change when it is updated and this report is reread later.]

<https://www.exploit-db.com/exploits/49735>

## 

## *High Severity Findings*

|  |  |
| --- | --- |
| Name | **01** |

## 

## *Medium Severity Findings*

|  |  |
| --- | --- |
| Name | **01** |

## 

## *Low Severity Findings*

|  |  |
| --- | --- |
| Name | **01** |

## *Informational Findings*

|  |  |
| --- | --- |
| Name | **01** |

|  |  |
| --- | --- |
|  | Appendix |

## [Appendix A](#_duo021fn5s9l): Vulnerability Severity Scales

***Note:*** *[Team Name] opts to use these custom categories rather than CVSS ratings, as conventional rating systems tend to misrepresent complex situations and do not afford the flexibility to best present information.*

|  |  |
| --- | --- |
| **Critical** | A vulnerability with trivial complexity that, if exploited, will cause severe and potentially irreparable damage to company data, systems, and assets. These are vulnerabilities that should be patched and remediated immediately. |
| **High** | A vulnerability that has low complexity and has potential to directly threaten sensitive information on affected systems. |
| **Medium** | A vulnerability that either has a higher attack complexity or requires the chaining together of multiple exploits in order to cause serious harm. |
| **Low** | A finding that is unlikely to cause any damage directly. However, a malicious actor could leverage information gathered from a vulnerability of this severity as part of a later exploit. |
| **Informational** | Information gathered that presents little to no threat to the system it is present on but should be noted or remediated to lessen the attack surface of the organization. |

## 

## 

## [Appendix B](#_m823gbvohlg9): Open-Source Intelligence

[Team Name] was able to find public information on the following employees. It may be desirable to limit the exposure or connection of these public accounts to the company to maintain a superior security posture.

#### **Social Media**

[LINK]



[LINK]



[LINK]



[LINK]



[LINK]

These accounts combined allowed *[Team Name]* to collect significant information, for example:

* [Credentials or whatever]

## [Appendix](#_duo021fn5s9l) C: Vulnerability Severity Scales

*[Team Name]* utilizes a custom version of the Penetration Testing Execution Standard, which is both intended for business and security specialist organizations, with a standardized language and set of operations for performing evaluations.

A diagram of a diagram

Description automatically generated with medium confidence