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.

|  |  |
| --- | --- |
|  | Table of Contents [REGEN THIS] |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Executive Summary | | |
| At the request of [Company Name], a penetration test was conducted on [specific scope/systems or features being tested]. This assessment was structured in two key stages to identify potential security vulnerabilities and assess the risk to critical assets. The first stage, pre-engagement operations, involved extensive open-source intelligence gathering to identify potential external risks. This was followed by the assessment phase, in which active reconnaissance and controlled exploitation techniques were employed to confirm the existence and potential impact of any identified vulnerabilities.  The following report provides a detailed overview of the findings from these engagement phases, along with targeted recommendations for remediation. In particular, the assessment focused on [mention specific critical systems or data assets relevant to the company], ensuring that these essential systems and data flows were carefully reviewed to uphold their security. This assessment was performed with adherence to relevant data protection laws and regulations, such as [mention specific laws like GDPR, HIPAA, etc., if pertinent], in order to align with compliance standards applicable to [Company Name]’s industry.  This summary includes a high-level overview of the key findings, presented in a visual chart that categorizes vulnerabilities by severity and frequency. This chart provides a quick reference to the most pressing issues, organized by risk level and their potential business impact. Additional details for each of these vulnerabilities can be found in the “Technical Findings” section. Following this, [Team Name] offers strategic insights for bolstering your organization’s security posture, with recommendations for both immediate action and long-term improvements.  [have num of vuln graph, and other graphs that are \*pretty\* and execs will eat up] | **Timeline**  Engagement  Began  *[Date Begin]*  Engagement  Concluded  *[Date end]* | |
| **Findings**  **N** Critical  **N** High  **N** Medium  **N** Low  **N** Informational | |

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]

|  |  |
| --- | --- |
|  | Engagement Outline |

Stuff like network map, what we did, how we did, scope, etc

Overview… blah blah

### 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]*.

|  |  |
| --- | --- |
| Network | CIDR/Address Space |
| NAME\_OF\_NETWORK | 0.0.0.0/0 |
| NAME\_OF\_NETWORK | 0.0.0.0/0 |
| NAME\_OF\_NETWORK | 0.0.0.0/0 |

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

[INSERT TABLE IF APPLICABLE]

### Network Diagram

[IMAGE\_OF\_NET\_DIAGRAM\_HERE – draw.io]

### Attack Narrative

Key steps walking through high points in attack. Basically a high level overview of what we did

### Sample Finding Walkthrough

The following is an example of a typical finding you’ll see in this report. This sample is provided to help you understand the formatting, structure, and detail included in each finding, allowing for a clearer interpretation of the report's layout and content. It illustrates how each vulnerability is documented, from the technical description to the business impact and recommended remediation steps.

|  |  |
| --- | --- |
| Example Finding Name  CVSS: Score - Severity | Score |

|  |  |  |  |
| --- | --- | --- | --- |
| Attack Vector: | Network | Local | Physical | Scope: | Unchanged | Changed |
| Attack Complexity : | **Low | High** | Confidentiality : | **None | Low | High** |
| Required Privileges : | **None | Low | High** | Integrity: | **None | Low | High** |
| User Interaction : | **None | Required** | Availability : | **None | Low | High** |

Each finding begins with a Title, CVSS Score, and Severity level, followed by a detailed breakdown of the CVSS metrics. For an in-depth explanation of these metrics, refer to [this guide on CVSS scores](https://www.balbix.com/insights/base-cvss-scores/).

#### **Description**

This section provides an in-depth explanation of the identified vulnerability, including its technical context and relevance. It clarifies the underlying cause of the issue, potential methods of exploitation, and the resulting impact, equipping you with a clear understanding of the risk presented.

#### **Affected Systems**

This section identifies the specific systems, applications, or network components impacted by the vulnerability. By detailing the affected areas, it enables you to understand the scope of exposure and prioritize remediation efforts accordingly.

#### **Observations**:

This section gives a step-by-step overview of the testing process, including screenshots, error messages, logs, or other outputs that confirm the vulnerability. Each observation is documented clearly to show exactly what was done and the results found during testing.

#### **Business Impact**

This section outlines the potential effects of the vulnerability on your organization, including risks to data security, operational disruptions, financial implications, and reputational damage. It translates the technical findings into clear business consequences, helping you understand the broader impact on your organization.

#### **Remediations**:

#### This section provides recommended actions to address and resolve the identified vulnerability. Each remediation step is designed to mitigate risks effectively, offering guidance on configuration changes, patches, code updates, or process improvements needed to secure affected systems and prevent similar issues in the future.

#### **References**

This section includes relevant resources and documentation that provide additional information on the vulnerability, remediation techniques, and best practices. References may consist of industry standards, vendor documentation, or research articles to support a deeper understanding and further exploration of the issue.

### Severity Ratings

|  |  |  |
| --- | --- | --- |
| Explanation | Vulnerability | CVSS Score |
| Vulnerabilities with a CVSS score of 9.0 to 10.0.  These vulnerabilities allow attackers to easily exploit the system, often remotely, and can lead to significant data loss, system compromise, or other severe consequences. Immediate remediation is required. | Critical | 9.0-10.0 |
| Vulnerabilities with a CVSS score of 7.0 to 8.9.  These present a serious risk to the organization and can be exploited by attackers to gain access to sensitive data or disrupt operations. Remediation should be prioritized. | High | 7.0-8.9 |
| Vulnerabilities with a CVSS score of 4.0 to 6.9.  While not immediately critical, these vulnerabilities may still be exploitable and could pose a risk over time or under certain conditions. They should be addressed in a reasonable timeframe. | Medium | 4.0-6.9 |
| Vulnerabilities with a CVSS score of 0.1 to 3.9.  These present a minimal risk and are typically harder to exploit. While they may not pose an immediate threat, they should still be remediated to avoid potential risks over time. | Low | 0.1-3.9 |
| These are not classified as vulnerabilities but are included to provide additional insights into the system or environment. No immediate action is required, but they may be useful for improving overall security posture. | Informational | 0.0 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Page | Risk | Vulnerability | CVSS Score |
| NUM | {#findings}{#cvss.baseSeverity == 'Critical'}{title} | {cvss.baseSeverity}  {/cvss.baseSeverity == 'Critical'} | {cvss.baseMetricScore}{/findings} |
| NUM | {#findings}{#cvss.baseSeverity == 'High'}{title} | {cvss.baseSeverity}  {/cvss.baseSeverity == 'High'} | {cvss.baseMetricScore}{/findings} |
| NUM | {#findings}{#cvss.baseSeverity == 'Medium'}{title} | {cvss.baseSeverity}  {/cvss.baseSeverity == 'Medium'} | {cvss.baseMetricScore}{/findings} |
| NUM | {#findings}{#cvss.baseSeverity == 'Low'}{title} | {cvss.baseSeverity}  {/cvss.baseSeverity == 'Low'} | {cvss.baseMetricScore}{/findings} |
| NUM | {#findings}{#cvss.baseSeverity == 'Informational'}{title} | {cvss.baseSeverity}  {/cvss.baseSeverity == 'Informational'} | {cvss.baseMetricScore}{/findings} |

{#findings}

|  |  |
| --- | --- |
| [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {title}  CVSS: {cvss.baseMetricScore} - {cvss.baseSeverity} | {@cvss.cellColor}  {cvss.baseMetricScore} |

|  |  |  |  |
| --- | --- | --- | --- |
| Attack Vector: | {cvssObj.AV} | Scope: | {cvssObj.S} |
| Attack Complexity : | **{cvssObj.AC}** | Confidentiality : | **{cvssObj.C}** |
| Required Privileges : | **{cvssObj.PR}** | Integrity: | **{cvssObj.I}** |
| User Interaction : | **{cvssObj.UI}** | Availability : | **{cvssObj.A}** |

### **Description**

{#description}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/description}

### 

### **Observations**

{#observation}

{@text | convertHTML}

{#images}

{%image}

Image 2 – {caption}

{/images}

{/observation}

### 

### **Affected Assets**

{@affected | convertHTML}

### **Business Impact**

### 

### **Remediation**

{#remediation}

{@text | convertHTML}

{#images}

{%image}

Image 3 – {caption}

{/images}

{/remediation}

### 

### **References**

{#references}

{.}

{/references}

{/findings}

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

### Open Source Intellegence

[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:

[TABLE WITH FINDINGS HERE THAT COULD BE RELEVANT]

##### Other Things:

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

### Thank You

We would like to extend our sincere appreciation to [COMPANY NAME] for the opportunity to conduct this penetration testing engagement. It has been a privilege to work with your team and assist in enhancing your organization's security posture.

Our goal was to identify potential vulnerabilities and provide actionable recommendations to help [COMPANY NAME] mitigate risks and strengthen its defenses against potential threats. We are confident that, by addressing the findings outlined in this report, [COMPANY NAME] will be well-equipped to maintain a more secure environment.

Thank you once again for entrusting us with this important work. If you have any questions or require further assistance, please do not hesitate to reach out to our team.