{{ company.name }}

Security Assessment Report Prepared For {{ client.name }}  


Report Issued: {{ report\_date }}

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to {{ client.name }} or facilitate attacks against {{ client.short\_name }}. {{ company.name }} shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on {{ client.name }}’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[Confidentiality Notice 1](#_heading=h.gjdgxs)

[Disclaimer 2](#_heading=h.30j0zll)

[EXECUTIVE SUMMARY 3](#_heading=h.1fob9te)

[<TODO Optional - Big Issue> Recommendation 4](#_heading=h.3znysh7)

[HIGH LEVEL ASSESSMENT OVERVIEW 4](#_heading=h.2et92p0)

[Observed Security Strengths 5](#_heading=h.tyjcwt)

[Areas for Improvement 5](#_heading=h.1t3h5sf)

[Short Term Recommendations 5](#_heading=h.4d34og8)

[Long Term Recommendations 5](#_heading=h.17dp8vu)

[SCOPE 5](#_heading=h.lnxbz9)

[Networks 6](#_heading=h.35nkun2)

[Other 6](#_heading=h.1ksv4uv)

[Provided Credentials 6](#_heading=h.44sinio)

[TESTING METHODOLOGY 6](#_heading=h.2jxsxqh)

[CLASSIFICATION DEFINITIONS 7](#_heading=h.3j2qqm3)

[Severity Classifications 7](#_heading=h.1y810tw)

[Exploitation Likelihood Classifications 7](#_heading=h.4i7ojhp)

[Business Impact Classifications 7](#_heading=h.2xcytpi)

[Remediation Difficulty Classifications 7](#_heading=h.1ci93xb)

[ASSESSMENT FINDINGS 7](#_heading=h.2bn6wsx)

[APPENDIX B - ENGAGEMENT INFORMATION 7](#_heading=h.qsh70q)

[{{ client.name }} Points Of Contact 7](#_heading=h.3as4poj)

[Version Information 7](#_heading=h.1pxezwc)

[{{ company.name }} Contact Information 7](#_heading=h.49x2ik5)

# EXECUTIVE SUMMARY

{{ company.name }} performed a security assessment of the internal corporate network of {{ client.name }} on {{ report\_date }}. {{ company.name }}’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within the {{ client.short\_name }} corporate network. The purpose of this assessment was to discover and identify vulnerabilities in {{ client.short\_name }}‘s infrastructure and suggest methods to remediate the vulnerabilities. {{ company.name }} identified a total of {{ totals.findings }} vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** | **INFORMATIONAL** |
| {{ totals.findings\_critical }} | {{ totals.findings\_high }} | {{ totals.findings\_medium }} | {{ totals.findings\_low }} | {{ totals.findings\_info }} |

The highest severity vulnerabilities give potential attackers the opportunity to <TODO BAD ACTIONS THAT COULD OCCUR HERE - FULL PARAGRAPH WITH HIGH-LEVEL DETAIL>. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## <TODO Optional - Big Issue> Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn’t a technical vulnerability but still should be brought to the attention of the executive team.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

{{ company.name }} identified the following strengths in {{ client.name }}’s network which greatly increases the security of the network. {{ client.short\_name }} should continue to monitor these controls to ensure they remain effective.

<TODO Strength Category>

* <TODO Individual Strength>

## Areas for Improvement

{{ company.name }} recommends {{ client.name }} takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack {{ client.short\_name }}’s information systems and/or reduce the impact of a successful attack.

### Short Term Recommendations

{{ company.name }} recommends {{ client.name }} take the following actions as soon as possible to minimize business risk.

<TODO Recommendation Category>

* <TODO Individual Recommendation>

### Long Term Recommendations

{{ client.name }} recommends the following actions be taken over the coming months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

<TODO Recommendation Category>

* <TODO Individual Recommendation>

# 

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

|  |  |
| --- | --- |
| **Network** | **Note** |
| {%tr for s in scope %} | |
| {% for line in s.scope -%}  {{ line }}  {%- endfor %} | {{ s.name }}{% if s.disallowed is true %} – **Out Of Scope**{% endif %}{% if s.requires\_caution is true %} – **Sensitive**{% endif %} |
| {%tr endfor %} | |

## Other

|  |  |  |
| --- | --- | --- |
| **Name** | **System Type** | **Note** |
| TODO | TODO | TODO |

## Provided Credentials

{{ client.name }} provided {{ company.name }} with the following credentials and access to facilitate the security assessment listed below.

|  |  |
| --- | --- |
| **Item** | **Note** |
| TODO | TODO |
| TODO | TODO |

# TESTING METHODOLOGY

{{ company.name }}’s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about {{ client.name }}’s network systems. {{ company.name }} used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. {{ company.name }} simulated an attacker exploiting vulnerabilities in the {{ client.short\_name }} network. {{ company.name }} gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.

# 

# CLASSIFICATION DEFINITIONS

## Severity Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

|  |  |
| --- | --- |
| **Difficulty** | **Description** |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

## 

# ASSESSMENT FINDINGS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number** | **Finding** | **Severity** | **Score** | **Page** |
| {%tr for finding in findings %} | | | | |
| {{ finding.position }} | {{ finding.title }} | {% cellbg finding.severity\_color %}{{ finding.severity }} | {% cellbg finding.severity\_color %} {{ finding.cvss\_score }} | TODO |
| {%tr endfor %} | | | | |

**{% for finding in findings %}**

**{{ finding.position }} - {{ finding.title }}**

|  |  |
| --- | --- |
| **{% cellbg finding.severity\_color %}{{ finding.severity }} ({{ finding.cvss\_score }}/10)** | |
| **Exploitation Likelihood** | **TODO** |
| **Business Impact** | **TODO** |
| **Remediation Difficulty** | **TODO** |

**Security Implication**

{{p finding.description\_rt }}

**Analysis**

{{p finding.impact\_rt }}

{% if finding.affected\_entities %}

**Affected Hosts**

{{p finding.affected\_entities\_rt }}

{% endif %}

**Recommendations**

{{p finding.recommendation\_rt }}

{% if finding.references %}

**References**

{{p finding.references\_rt }}

{% endif %}

{% endfor %}

APPENDIX A - PASSWORD DATA

|  |  |
| --- | --- |
| **Easy Passwords** | All passwords discovered can be found on publicly accessible wordlists. Even if passwords were found in a hashed state, they can be cracked in a minimal amount of time. |
| **Password Length** | No minimum password length was set. Many passwords had less than 8 characters, which is the standard for password length. NIST recommends a minimum length of 12 characters. |
| **Reverse Encyrption** | Passwords were stored with reversible encryption on Active Directory. Domain administrators can easily reverse hashed credentials back to cleartext passwords without a key. This should be disabled. |

APPENDIX B - TOOLS USED

|  |  |
| --- | --- |
| **TOOL** | **DESCRIPTION** |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Metasploit** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **BloodHound** | Used for Active Directory Enumeration |
| **Sliver** | Used for command and control, and to host the phishing campaign payload |
| **TODO** | TODO |

# APPENDIX C - ENGAGEMENT INFORMATION

## {{ client.name }} Points Of Contact

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| {%tr for poc in client.contacts %} | | |
| {{ poc.name }} | {{ poc.job\_title }} | {{ poc.email }}{% if poc.phone %} - {{ poc.phone }}{% endif %} |
| {%tr endfor %} | | |

## Version Information

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | {{ report\_date }} | Initial report to client |

## {{ company.name }} Contact Information

|  |  |
| --- | --- |
| **Name** | {{ company.name }} Consulting |
| **Address** | 1001 Fake Street, Gotham, NY 11201 |
| **Phone** | 778-330-2389 |
| **Email** | <TODO REPLACE WITH PROVIDED EMAIL> |