## 

ACME Security Company

**<TARGET COMPANY>**

**Internal Penetration Test**

**Report of Findings**

<TARGET COMPANY>

<DATE>

Version 1.

**Table of Contents**

[Statement of Confidentiality 3](#_Toc126460053)

[Engagement Contacts 4](#_Toc126460054)

[Executive Summary 5](#_Toc126460055)

[Approach 5](#_Toc126460056)

[Scope 6](#_Toc126460057)

[Assessment Overview and Recommendations 6](#_Toc126460058)

[Network Penetration Test Assessment Summary 7](#_Toc126460059)

[Summary of Findings 7](#_Toc126460060)

[Internal Network Compromise Walkthrough 8](#_Toc126460061)

[Detailed Walkthrough 8](#_Toc126460062)

[Remediation Summary 9](#_Toc126460063)

[Short Term 9](#_Toc126460064)

[Medium Term 9](#_Toc126460065)

[Long Term 9](#_Toc126460066)

[Technical Findings Details 10](#_Toc126460067)

[Appendices 11](#_Toc126460068)

[Appendix A – Finding Severities 11](#_Toc126460069)

[Appendix B – Exploited Hosts 12](#_Toc126460070)

[Appendix C – Compromised Users 13](#_Toc126460071)

[Appendix D – Changes/Host Cleanup 14](#_Toc126460072)

# Statement of Confidentiality

The contents of this document have been developed by ACME Security Company. ACME Security Company considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from ACME Security Company. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of ACME Security Company.

The contents of this document do not constitute legal advice. ACME’s offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect the targets external or internal infrastructure.

# Engagement Contacts

|  |  |  |
| --- | --- | --- |
| **<TARGET COMPANY> Contacts** | | |
| **Primary Contact** | **Title** | **Primary Contact Email** |
| Marcellus Edson | Chief Executive Officer | medson@<TARGET COMPANY>.com |
| **Secondary Contact** | **Title** | **Secondary Contact Email** |
| Mildred Day | Chief Technical Officer | mday@<TARGET COMPANY>.com |

|  |  |  |
| --- | --- | --- |
| **Assessor Contact** | | |
| **Assessor Name** | **Title** | **Assessor Contact Email** |
| ACME Security Company | Security Consultant | acme@acme.com |

# Executive Summary

<TARGET COMPANY> (“<TARGET>” herein) contracted ACME Security Company to perform a Network Penetration Test of <TARGET>’s internally facing network to identify security weaknesses, determine the impact to <TARGET>, document all findings in a clear and repeatable manner, and provide remediation recommendations.

## Approach

ACME Security Company performed testing under a “black box” approach on <DATE> without credentials or any advance knowledge of <TARGET>’s internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely via a host that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. ACME Security Company sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If ACME Security Company were able to gain a foothold in the internal network, <TARGET> would allow for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

## Scope

The scope of this assessment was <DESCRIBE SCOPE>

In-Scope Assets

|  |  |
| --- | --- |
| **HOST/URL/IP Address** | **Description** |
| <IP ADDRESS> | <DESCRIPTION> |

*Table 1: Scope Details*

## Assessment Overview and Recommendations

<ASSESSMENT>

# Network Penetration Test Assessment Summary

Hack The Box Academy began all testing activities from the perspective of an unauthenticated user on the internal network. <TARGET> provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

## Summary of Findings

During the course of testing, ACME Security Company uncovered a total of <NUMBER> findings that pose a material risk to <TARGET>’s information systems. ACME Security Company also identified one informational finding that, if addressed, could further strengthen <TARGET>’s overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

|  |  |  |  |
| --- | --- | --- | --- |
| Finding Severity | | | |
| High | Medium | Low | Total |
|  |  |  |  |
|  |  |  |  |

*Table 2: Severity Summary*

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

|  |  |  |
| --- | --- | --- |
| **Finding #** | **Severity Level** | **Finding Name** |
|  |  |  |
|  |  |  |

*Table 3: Finding List*

# Internal Network Compromise Walkthrough

<DETAILED OVERVIEW>

## Detailed Walkthrough

<DEATILED WALKTHROUGH WITH SCREENSHOTS>

# Remediation Summary

As a result of this assessment there are several opportunities for <TARGET> to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. <TARGET> should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

## Short Term

## Medium Term

## Long Term

# Technical Findings Details

1. <TECHNICAL FINDING> - <CRITICALITY>

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score |  |
| Description (Incl. Root Cause) |  |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

# Appendices

## Appendix A – Finding Severities

Each finding has been assigned a severity rating of high, medium, or low. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of <TARGET>’s data.

|  |  |
| --- | --- |
| **Rating** | **Severity Rating Definition** |
| **High** | Exploitation of technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited. |
| **Medium** | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR –  The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |
| **Low** | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR –  The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |

*Table 4: Severity Definitions*

## Appendix B – Exploited Hosts

|  |  |  |  |
| --- | --- | --- | --- |
| **Host** | **Scope** | **Method** | **Notes** |
|  |  |  |  |
|  |  |  |  |

*Table 5: Exploitation Attempt Details*

## Appendix C – Compromised Users

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | **Type** | **Method** | **Notes** |
|  |  |  |  |
|  |  |  |  |

*Table 6: User Accounts Compromised*

## Appendix D – Changes/Host Cleanup

|  |  |  |
| --- | --- | --- |
| **Host** | **Scope** | **Change/Cleanup Needed** |
|  |  |  |
|  |  |  |

*Table 7: Assessment Artifacts*