{Name}

Security audit report of <PRODUCTS>

COMPANY LOGO HERE

CONFIDENTIAL   
DO NOT DISTRIBUTE

Table of Contents

Executive Summary……………………………………..……………………………………………………pg #

Impact Analsys………………….……………..…………………………….…………………………………pg #

Engagement Overview…………………………………………..……..……………………………………pg #

Network Topology………..…………………………...….…………………………………………pg #

Methodology……………………………………………………………………………………………pg #

Technical Findings…………………………………………………….………………………………………pg #

Critical Severity Findings………………………………….………………………………………pg #

High Severity Findings……………………………..….….………………………………………pg #

Medium Severity Findings……………………………..…………………………………………pg #

Low Severity Findings………………………………….….……….………………………………pg #

Appendix……………………………………..……………..……….….……….………………………………pg #

Appendix A: Vulnerability Severity Scale (CVSS) ……….………………………………pg #

Appendix B: Tools used……………..…………………………………………………………….pg #

Executive Summary

ADD SUMMARY HERE. This should be brief and share little to zero technical details and highlight more business risks, security risks, and product risks. Include vulnerabilities found but do not go into detail about them. Little information may be provided but it is better to add more detail in the technical summary. Should be on its own page so it may be given to a CTO, CEO or other executive for a quick run-down to save time and not cause confusion.

Impact Analysis

Talk about what impact your findings have, which assets are most impacted, give general recommendations, and a somewhat technical summary of vulnerabilities that's meant to show the bigger picture. Focus should be on the data & assets. Note from Jibran: I'm having a hard time understanding why we need both an impact analysis and an executive summary

**METHODOLOGY:**

will be the overall approach of the pentest. So basically, explain what your first to last steps are. So explain what each phase of your attack is. Should be a conversation about how you avoided breaking machines. (formulate methodology around Pen Testing Execution Standard)

**Technical Findings**

**Critical Severity Findings**

**{Name of Finding}  
{Scope}  
{Description}**

**Maybe some images????**

**{Impact}  
{Remediation}  
{References}**

**High Severity Findings**

**{Name of Finding}  
{Scope}  
{Description}**

**Maybe some images????**

**{Impact}  
{Remediation}  
{References}**

**Medium Severity Findings**

**{Name of Finding}  
{Scope}  
{Description}**

**Maybe some images????**

**{Impact}  
{Remediation}  
{References}**

**Low Severity Findings**

**{Name of Finding}  
{Scope}  
{Description}**

**Maybe some images????**

**{Impact}  
{Remediation}  
{References}**

APPENDIX

The appendix will cover the scale system that we used and our tools.

**Appendix A:**

Explain the scaling system we reference as our guide (the CVSS) and explain our thought process behind how we listed vulnerabilities

**Appendix B:**

Explain all the tools used and a very very short explanation of what it does

**Original feedback from meeting:**

Overall Feedback:   
- Should have a clearly visible disclosure about confidentiality and a smaller footnote reminding you of this (about document sensitivity)

**- (look for any official documentation from hurricane labs).**

**-** Blackhill might have video explaining how to write a good report

- We should be grouping exploits by assets and services

- Explain your thought process behind how you listed vulnerabilities

- Do Sashanks exercise on writing the “mini” 15 page report, will make when2meet after aking Felix

Updated Plan:

- Title Page

- Table of contents

- Executive Summary

- Impact Analysis: Talk about what impact your findings have, which assets are most impacted, give general recommendations, somewhat technical summary of vulnerabilities that's meant to show the bigger picture. Focus should be on the data & assets.

- Methodology, will be the overall approach of the pentest. So basically, explain what your first to last steps are. So explain what each phase of your attack is. Should be conversation about how you avoided breaking machines. (formulate methodology around Pen Testing Execution Standard)

- Should be links that take you to each exploit and a link to send you back. Should be very very clear its a link.

\*\*\*Big Technical Section\*\*\*

- List every exploitation in order of CVSS rating (or some official scoring method)