Company Name

Penetration Test

# Document Control

The first page of this document should be the cover page that contains the organisation’s logo and the type of test.

In this section include the reporter’s name, their role, and a method of contacting them (Email, work No., etc). Additionally, it is best to write the version control and document properties inside of tables to allow a user to quickly locate the information they require without having to read a paragraph of information.

Finally, do not include an introduction section about your organisation since this can be distracting from the main content of the report and a brief introduction should be done in the executive summary.

# Executive Summary

Summary of important findings within report While also being accessible for an executive level individual. Ensure this is a maximum of 2 paragraphs of information and no more. Beyond 2 paragraphs the executive summary becomes more of an essay to read and is no longer fit for purpose.

Contents

[Executive Summary 2](#_Toc157590951)

[Document Control 3](#_Toc157590952)

[Overview of Penetration Test 5](#_Toc157590953)

[Scope of Work 5](#_Toc157590954)

[Project Objectives 5](#_Toc157590955)

[Timeline 5](#_Toc157590956)

[Summary of Findings 5](#_Toc157590957)

[Summary of recommendations 5](#_Toc157590958)

[Overview of Methodology 6](#_Toc157590959)

[Reporting 6](#_Toc157590960)

[Detailed findings 7](#_Toc157590961)

[Critical Vulnerabilities 7](#_Toc157590962)

[Vulnerability 7](#_Toc157590963)

[High Vulnerabilities 9](#_Toc157590964)

[Vulnerability 9](#_Toc157590965)

[Medium Vulnerabilities 9](#_Toc157590966)

[Vulnerability 9](#_Toc157590967)

[Low Vulnerabilities 9](#_Toc157590968)

[Vulnerability 9](#_Toc157590969)

[Appendix 10](#_Toc157590970)

[Glossary 11](#_Toc157590971)

# Overview of Penetration Test

## Scope of Work

IP Addresses to be tested, type of pen test. The IP addresses should be inserted into a table for ease of access.

## Project Objectives

Provide the objectives that the organization will gain after knowing the risks related to the penetration of the target IP addresses/ system or application and what they will get after mitigating these risks by implementing the recommendations in the penetration testing report.

## Timeline

Testing duration

The tested IP address's risks, from pen-testing point of view, during the testing period only. The pen-tester does not hold any responsibilities if some risk aroused after this period due to some changes in the target systems.

## Summary of Findings

In a glance view show the number of discovered risks based on priorities.

Avoid language that are overly frightening. The best method of including this information would be to write up a table of the vulnerabilities with their impact to the organisation and risk evaluation. Additionally including a bar chart or a pie chart of the vulnerabilities based on their risk rating would be recommended.

## Summary of recommendations

Based on the analysis of risks and the high-level finding, the high-level recommendation for the target organization needs to be described. The best method of including this information is make a sub heading of each vulnerability in order of risk and give a concise summary of how to mitigate the vulnerability that is easy to read and simple to understand.

# Overview of Methodology

This section provides the needed information about how the penetration testing was conducted. What steps have been followed to collect the information, analyze it, the risk rating methodology used to calculate the risk for each piece of vulnerability, and it may also contain the tools that the pen-tester used for each stage.

## Reporting

This section should provide the client the information required to understand how the vulnerabilities obtained their vulnerability classification and what factors were considered such as CVSS score using not just the base score but including the environmental and temporal scores as well.

# Detailed findings

This section provides detailed information for each finding. Present the findings in the simplest way as possible.

Critical Vulnerabilities

Vulnerability

#### Description

For each piece of vulnerability, a clear description should be given about the source of the vulnerability, its impact, and the likelihoods of the vulnerability to be exploited. Report should explain the source of the vulnerability and the root cause of the problem not the symptom of it. Additionally include images if it aids the client in understanding where the vulnerability was caused.

#### Impact

The report should explain the impact of the vulnerability's exploitation by the threat agent.

#### Likelihood

The report should state the likelihood of a vulnerability being exploited by the threat source (e.g. a hacker). Practical penetration tester may think of the likelihood as a combination of ease of access,

level of access gained, difficulty of discovering the vulnerability and exploiting it,

and the value of the asset to the target organization.

#### Risk Evaluation

Process of comparing the estimated risk against given risk criteria to determine the significance of the risk. There is many methods to doing this, a recommended method would be to use the CVSS scoring system.

#### Recommendation

Based on the risk rating and the target asset, the penetration tester should provide an acceptable recommendation with alternatives. For example, for weak authentication protocols being used to validate accounts for accessing a customer database through the ASP Web application, pen tester may provide more than option for mitigating the risk such as: 1-Implement Public Key Infrastructure (PKI) by providing certificate to all users of the database and require certificate-based authentication on the front-end. Additionally include screenshots or commands if it aids the client in understanding how to mitigate the vulnerability. When adding commands, use the “Commands” style which has been created specifically to make the information stick out from the rest of the recommendation.

Sample Command

#### References

Include external links that relate to a piece of information within the vulnerability to give a wider context to the reader and allow for additional research from the sources they have used. Give each reference a small sentence explaining what additional value the reference gives.

High Vulnerabilities

Vulnerability

#### Description

#### Impact

#### Likelihood

#### Risk Evaluation

#### Recommendation

#### References

Medium Vulnerabilities

Vulnerability

#### Description

#### Impact

#### Likelihood

#### Risk Evaluation

#### Recommendation

Low Vulnerabilities

Vulnerability

#### Description

#### Impact

#### Likelihood

#### Risk Evaluation

#### Recommendation

# Appendix

An appendix contains additional information related to the report, but which is not essential to the main findings. This can be consulted if the reader wishes to, but the report should not depend on this. Such information may include the scanning result, vulnerability assessment results, or other information, which may be useful for the reader. It is recommended to separate the Appendix into multiple Appendix sections (Appendix A, Appendix B, Appendix C, etc).

# Glossary

Define the meaning of technical terms which may be confusing to an individual that is not in cyber-security specifically. It would be best to make a bullet point kind of list with the definition under it to allow for an individual to quickly find the definition they are looking for.