Penetration Test Report

for

DinoBank

<Team name here>

<Report Date here>

**Table of Contents**

Table of Contents

[Executive Summary 4](#_Toc21445904)

[Overview of penetration testing process 5](#_Toc21445905)

[Overview of FFIEC Cybersecurity Assessment Tool 6](#_Toc21445906)

[Overview of findings 7](#_Toc21445907)

[Assessment Factor: Preventative Controls 7](#_Toc21445908)

[Infrastructure Management – Status: Baseline 7](#_Toc21445909)

[Access and Data Management – Status: Evolving 7](#_Toc21445910)

[Device/End-Point Security 7](#_Toc21445911)

[Secure Coding 7](#_Toc21445912)

[Assessment Factor: Detective Controls 7](#_Toc21445913)

[Threat and Vulnerability Detection 7](#_Toc21445914)

[Anomalous Activity Detection 7](#_Toc21445915)

[Event Detection 7](#_Toc21445916)

[Assessment Factor: Corrective Controls 7](#_Toc21445917)

[Patch Management 7](#_Toc21445918)

[Remediation 7](#_Toc21445919)

[Technical Summary 8](#_Toc21445920)

[Operating Systems Security issues 8](#_Toc21445921)

[Details of findings 8](#_Toc21445922)

[Recommendation and fixes 8](#_Toc21445923)

[Annexes 9](#_Toc21445924)

[Nessus scan results 9](#_Toc21445925)

[Nmap scan results – Linux server 9](#_Toc21445926)

[Nmap scan results – Windows server 9](#_Toc21445927)

[Linux Firewall verification 9](#_Toc21445928)

[Linux Apparmor verification 9](#_Toc21445929)

[References 10](#_Toc21445930)

# Executive Summary

*This section should be brief and non-technical in nature, not more than 1 page in total.*

# Overview of penetration testing process

# Overview of FFIEC Cybersecurity Assessment Tool

# Overview of findings

## Assessment Factor: Preventative Controls

### Infrastructure Management – Status: Baseline

Blah blah blah

### Access and Data Management – Status: Evolving

Blah blah blah

### Device/End-Point Security

### Secure Coding

## Assessment Factor: Detective Controls

### Threat and Vulnerability Detection

### Anomalous Activity Detection

### Event Detection

## Assessment Factor: Corrective Controls

### Patch Management

### Remediation

# Technical Summary

*Discuss the various issues discovered, in a very technical detail.*

## Operating Systems Security issues

### Details of findings

*Give specific details of issues found for the particular subsection. If multiple issues are discovered, make sure to clearly enumerate them.*

### Recommendation and fixes

*Give specific details for recommendations to remediate the issues discussed in the previous subsection. For each issue discussed above, there should be an accompanying recommendation and/or fix.*

# Annexes

*Annexes should be individually titled using the “Heading 2” format.*

## Nessus scan results

*The “Summary” and “Details” section of the scan of both systems should be located here. This should display the breakdown of all vulnerabilities discovered by ranking, as well as the associated detail content of the Nessus report.*

## Nmap scan results – Linux server

*A screencap of an Nmap scan of the Linux server, showing IP address and state of required services*

## Nmap scan results – Windows server

*A screencap of an Nmap scan of the Windows server, showing IP address and state of required services*

## Linux Firewall verification

*A screencap of the default state of the INPUT chain, along with all rules contained in the chain*

## Linux Apparmor verification

*A screencap of the Apparmor status of the Linux server*

# References

*References should be in APA format*