Submitted to: Application Development Team  
Security Analyst: Udacity Student  
  
Date of Testing: 4 July 2025  
Date of Report Delivery: 4 July 2025



|  |
| --- |
| Template |

**Table of Contents**

[Security Engagement Summary 2](#_Toc172710766)

[Engagement Overview 2](#_Toc172710767)

[Scope 2](#_Toc172710768)

[Risk Analysis 2](#_Toc172710769)

[Recommendations 2](#_Toc172710770)

[Significant Vulnerabilities Summary 4](#_Toc172710771)

[High-Risk Vulnerabilities 4](#_Toc172710772)

[Medium-Risk Vulnerabilities 4](#_Toc172710773)

[Low-Risk Vulnerabilities 4](#_Toc172710774)

[Significant Vulnerability Details 4](#_Toc172710775)

[Appendix A: Security Analysis Methodology 6](#_Toc172710776)

[Assessment Tools Selection 6](#_Toc172710777)

[Reconnaissance 7](#_Toc172710778)

[Scanning 7](#_Toc172710779)

[Exploitation 7](#_Toc172710780)

# Security Engagement Summary

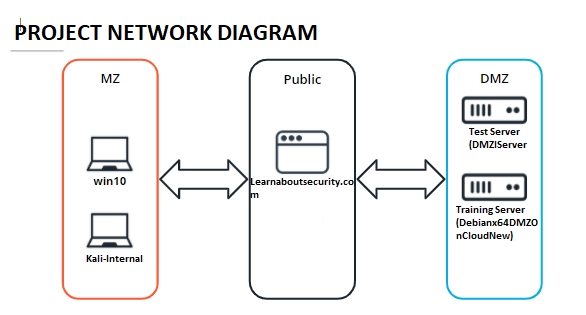
## Engagement Overview

The engagement has been conducted in order to determine the security posture of PJ Bank’s virtual environment and to highlight any security risks associated with the infrastructure in scope.

## Scope

The following devices are in scope of the assessment:

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Asset Information | Hostname | IP Address |
| 1 | Public web server | Learnaboutsecurity.com |  |
| 2 | Employee Workstation | Win10 | 10.1.2.4 |
| 3 | Debian Server in DMZ | DMZiServer | 10.1.0.7 |
| 4 | Web App Server in DMZ | Debianx64DMZOnCloudNew | 10.1.0.11 |



## Risk Analysis

<Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is **<DEFINE SEVERITY HERE as Low Moderate or High>.**

* **High** – severe or catastrophic impact
* **Moderate** – Serious impact
* **Low** – limited impact

>

## Recommendations

<Complete this section with recommendations based on major vulnerabilities discovered and/or exploited. The vulnerabilities highlighted in this report should be remediated as soon as possible>

* <Make non-technical and high level recommendations for an executive team to review. The recommendations should include things that executive-level directors, board members, and if provided to the public, someone non-technical can understand.

For example: The company should implement a policy that enforces multi-factor authentication. The security analysts determined that account passwords could be guessed and access to the network was gained remotely. Implementing multi-factor authentication would have prevented the analyst from gaining access to the network in this manner.>

# Significant Vulnerabilities Summary

Significant vulnerabilities identified during the vulnerability assessment and validation are summarized below. While additional vulnerabilities may be present, these are considered significant and warrant resolution.

## High-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

## Medium-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

## Low-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

# Significant Vulnerability Details

*Details about the significant vulnerabilities you listed above are provided below.*

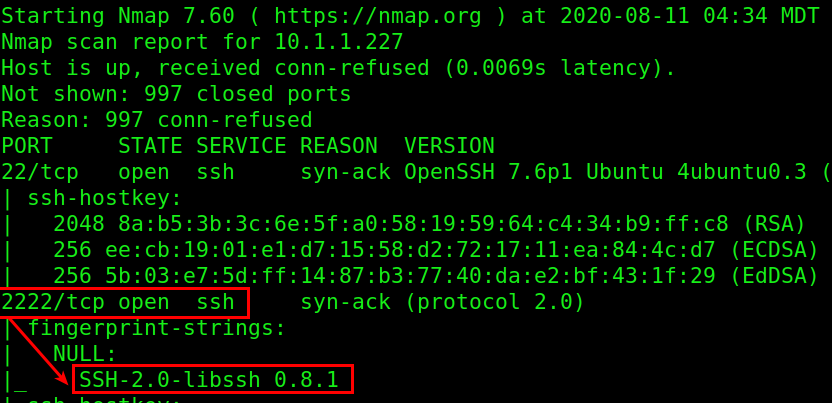
<For each vulnerability, make sure to:

* Identify the risk priority
* Describe the vulnerability
* Provide a screenshot that is centered, bordered, and has a caption
* Add a Discussion section under the screenshot>

Example of a vulnerability finding:

**HIGH-RISK Vulnerability**

The student found that both the LibSSH and Elasticsearch packages contained vulnerabilities directly associated with the lack of patching.



**Example of a machine with LibSSH Missing Software Patches**

Discussion:

<In your discussion, be sure to mention:

* Vulnerabilities were discovered <in what? why?>
* Are there any links available to discuss?

# Appendix A: Security Analysis Methodology

The methodology the analyst used for the vulnerability assessment is provided below.

## Assessment Tools Selection

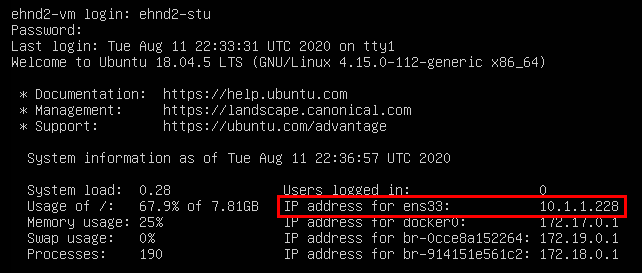
Noting the scope of the engagement was focused on a web application, the security analyst chose relevant web-application security analyst tools. The analyst created a Kali Virtual Machine which had many included tools. Tools used during this engagement included:

* Kali Operating System
  + <https://www.kali.org/>
  + Description
* Python Environment
  + <https://www.python.org/>
  + Description
* Nmap
  + <https://nmap.org/>
  + Description
* Others
  + Link
  + Description

Example:

Description of what/why you did

* Command used



**Screenshot of <COMMAND> and results**

### 

## Reconnaissance

<Provide a screenshot from the OSINT tool, and a description of the findings>

<DNS Information, including at least the names to IP mappings>

<Web technologies used by the website, with a screenshot of the identification >

## 

## Scanning

<Annotated screenshot and description of the nmap scans of each machine, one-by-one.>

## Exploitation

<Successful exploits to gain access/ exfiltrate sensitive data>

<Exploit commands>

<Vulnerable software exploitation>

<Weak Password Cracks>

<provide the commands you used and screenshots for them, with the description as seen in the example>

### 