Submitted to: Application Development Team  
Security Analyst: Udacity Student  
  
Date of Testing: Enter Date Here  
Date of Report Delivery: Enter Date Here



|  |
| --- |
| Template |

**Table of Contents**

[Security Engagement Summary 2](#_Toc67660169)

[Engagement Overview 2](#_Toc67660170)

[Scope 2](#_Toc67660171)

[Risk Analysis 2](#_Toc67660172)

[Recommendations 2](#_Toc67660173)

[Significant Vulnerabilities Summary 3](#_Toc67660174)

[High Risk Vulnerabilities 3](#_Toc67660175)

[Significant Vulnerability Details 3](#_Toc67660176)

[Appendix A: Security Analysis Methodology 4](#_Toc67660177)

[Assessment Tools Selection 4](#_Toc67660178)

[Red Team Operations Assessment 5](#_Toc67660179)

[Reconnaissance 5](#_Toc67660180)

[Scanning 5](#_Toc67660181)

[Exploit Development 5](#_Toc67660182)

# Security Engagement Summary

## Engagement Overview

<Provide a brief overview here. This should offer some background information about the Organization and describe the project objective. Use some of the language in the project instructions here.>

## Scope

<Define the scope here. List the target devices that you will pentest, identify their attributes such as hostname, IP address. Provide screenshots where helpful >

## 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

## Significant Vulnerability Details

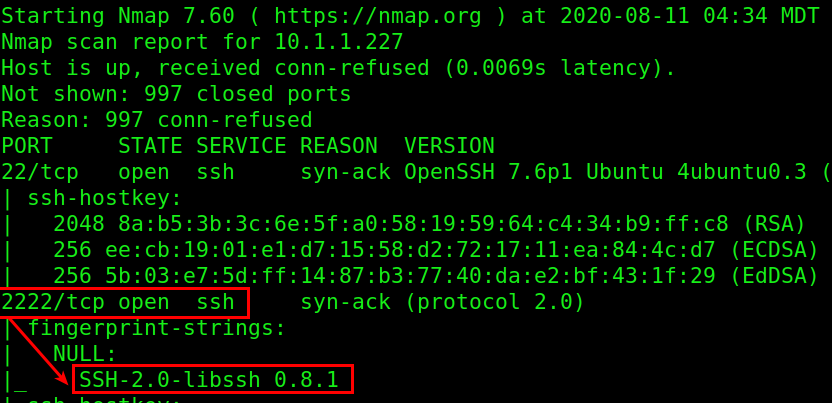
*<Details about the significant vulnerabilities you listed above are provided below.>*

**HIGH RISK**

<Tell us more, and make sure the effort could be replicated. What commands were used? What was found? Make sure to detail ALL identified significant vulnerabilities.>

Example:

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?

This concludes the Significant Vulnerability Detail portion of this report.>

# Appendix A: Security Analysis Methodology

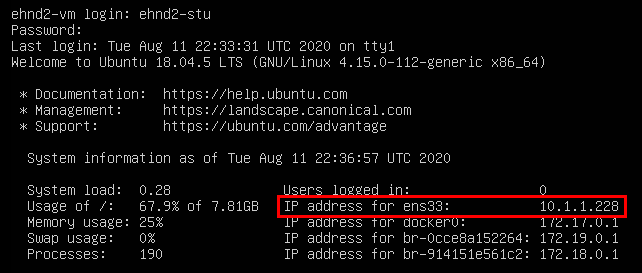
The methodology the analyst used for the vulnerability assessment is provided below.

**<Describe the target machine details here>**

Example:

The student launched the provided VM and noted the IP address after booting.

* System IP Address: **< LIST IP HERE >**



**Example: Console Screen of Application Virtual Machine**

## Assessment Tools Selection

**<Add tools and notes in the section below, as used>**

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

## Red Team Operations Assessment

<Enter an introductory paragraph here. This sections below is where you detail everything worth discussion from the project>

### Reconnaissance

<Describe Pen test starting point>

<reconnaissance investigations>

<findings: Any major Finding (if any should be Copied to the Significant Vulnerability Details Section of this report>

## 

### Scanning

<version scanning>

<vulnerability investigations and research findings>

<findings: Any major Finding (if any should be Copied to the Significant Vulnerability Details Section of this report>

### Exploit Development

<Successful exploits to gain access/ exfiltrate sensitive data>

<Exploit commands>

<Vulnerable software exploitation”

<Weak Password Cracks>

<findings: Any major Finding (if any should be Copied to the Significant Vulnerability Details Section of this report>

### 