



|  |
| --- |
| Template |

**Table of Contents**

[Security Engagement Summary 1](#_30j0zll)

[Engagement Overview 2](#_3znysh7)

[Scope 2](#_tyjcwt)

[Risk Analysis 2](#_1t3h5sf)

[Recommendations 2](#_4d34og8)

[Significant Vulnerabilities Summary **2**](#_lnxbz9)

[High-Risk Vulnerabilities 3](#_35nkun2)

[Medium-Risk Vulnerabilities 3](#_gug9fgvbagk5)

[Low-Risk Vulnerabilities 3](#_b1mp9hza0ye7)

[Significant Vulnerability Details 3](#_1ksv4uv)

[Appendix A: Security Analysis Methodology 5](#_4i7ojhp)

[Assessment Tools Selection 5](#_2xcytpi)

[Red Team Operations Assessment 6](#_1ci93xb)

[Reconnaissance 6](#_3whwml4)

[Scanning 6](#_qsh70q)

[Exploitation 7](#_3as4poj)

# 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, and identify their attributes such as hostname, and 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

<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.*

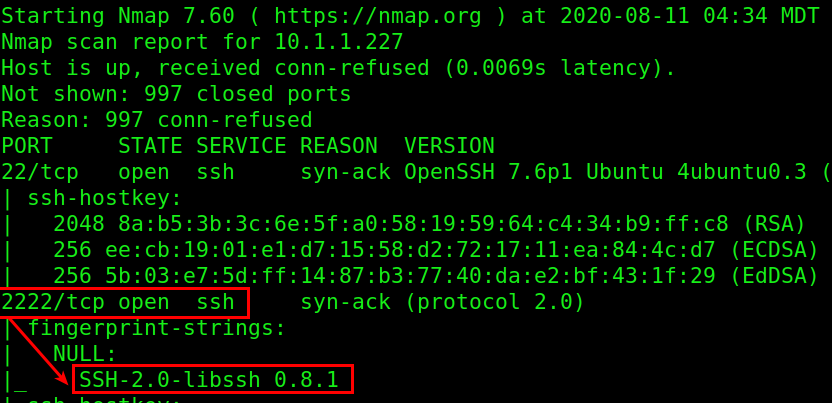
<For each vulnerability, make sure to:

* 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

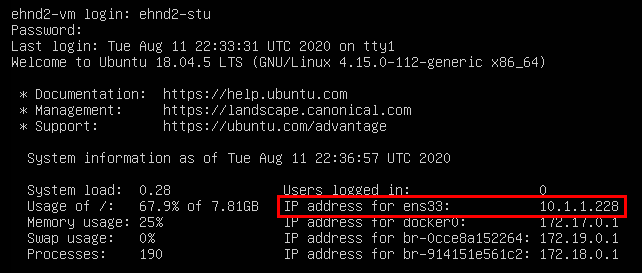
The methodology the analyst used for the vulnerability assessment is provided below.

**<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

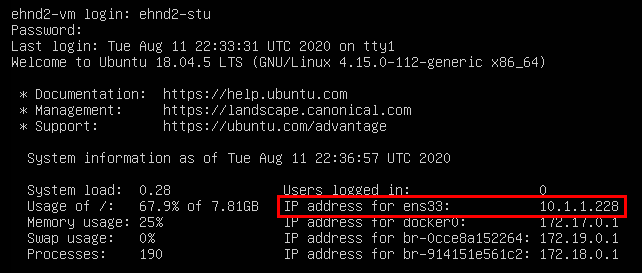
## Red Team Operations Assessment

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

Example:

Description of what/why you did

* Command used



**Screenshot of <COMMAND> and results**

### 

### Reconnaissance

<Describe Pen test starting point>

<reconnaissance investigations>

<findings: Any major finding from the website should be here>

## 

### Scanning

<version scanning on the VMs>

<vulnerability investigations and research findings of the VMs>

<provide the commands you used and screenshots for the scan, and describe any major findings as seen in the example>

### 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>

### 