Submitted to: Application Development Team  
Security Analyst: Tran Thang  
  
Date of Testing: 04/09/2023  
Date of Report Delivery: 04/09/2023



|  |
| --- |
|  |

**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

This engagement involved conducting a comprehensive penetration testing and red teaming assessment for the target organization, Learn About Security. The primary objective of this engagement was to identify vulnerabilities and weaknesses in the organization's systems, networks, and applications, and to provide actionable recommendations for improving their overall security posture.

## Scope

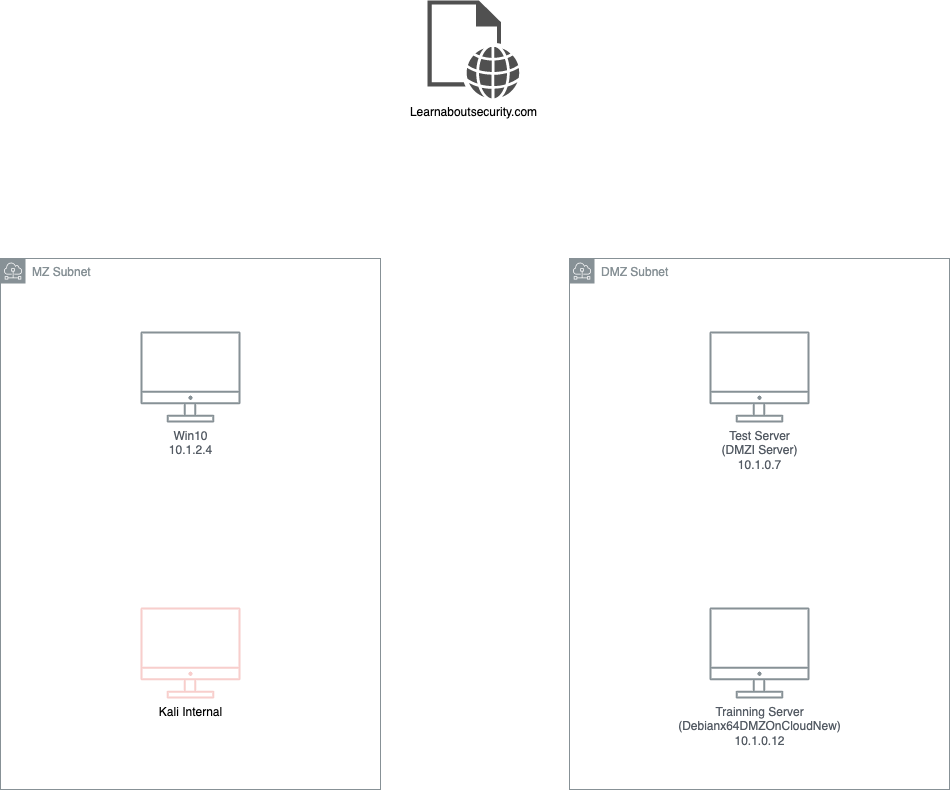
This engagement's scope included assessing the organization's external-facing infrastructure, internal network, and web applications. The assessment focused on identifying potential entry points, vulnerabilities, and misconfigurations that could be exploited by malicious actors. The assessment did not include any attempts to cause disruption or damage to the organization's systems.

Figure : The infrastructure resources we can do pen test on

## Risk Analysis

The evaluation helps in understanding the overall risk posture and enables informed decision-making regarding risk mitigation strategies.

During risk analysis rate evaluation, various factors are considered, such as the value of the assets at risk, the likelihood of a threat occurring, the potential impact of a successful attack, and the effectiveness of existing security controls. By quantifying and prioritizing risks, organizations can allocate resources effectively and implement appropriate countermeasures to reduce the overall risk level.

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

## Recommendations

# To be done

# 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

## Medium-Risk Vulnerabilities

## Low-Risk Vulnerabilities

# Significant Vulnerability Details

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

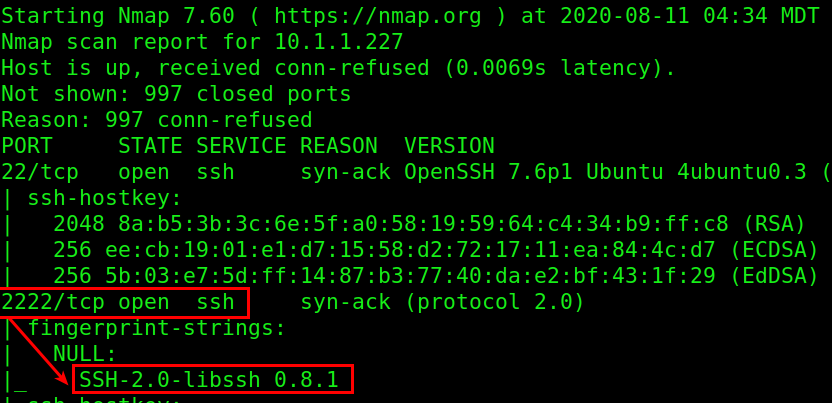
<For each vulnerability, make sure to:

* 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

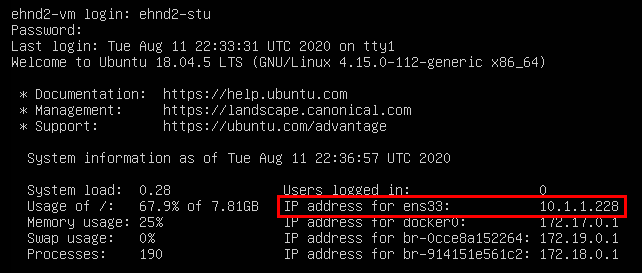
The methodology the analyst used for the vulnerability assessment is provided below.

**<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

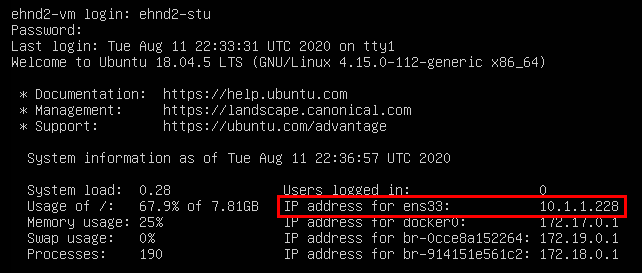
## Red Team Operations Assessment

<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

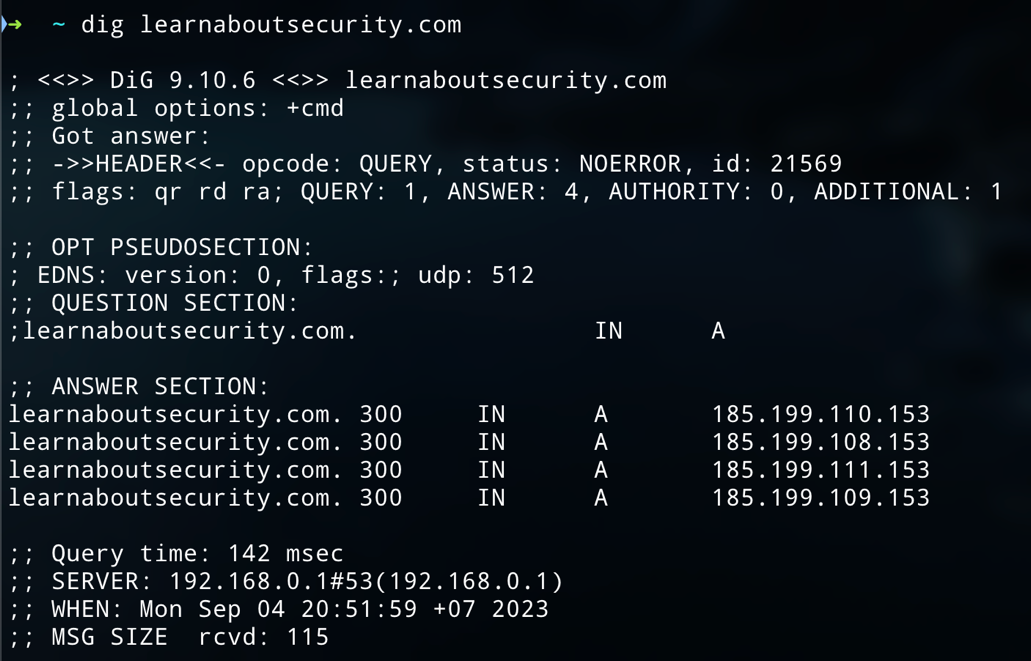


**Screenshot of <COMMAND> and results**

### 

### Reconnaissance

1. Investigate on <https://learnaboutsecurity.com/> page

4 Ips:

* 185.199.110.153
* 185.199.108.153
* 185.199.111.153
* 185.199.109.153

A screenshot of a computer

Description automatically generatedLocation: (Using Iana.org) is RIPE NCC -> Europe, Middle East, and Central Asia

Shodan search:

* A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generatedThe system is open with port 80 and 443 and there are some vulnerabilities.

Techstack scanning with wappalyzer:

### A screenshot of a computer Description automatically generatedA screenshot of a black screen Description automatically generated

### 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>

### 