**B**

TALHA SECURITY, Inc.

Security Assessment Report Template

Date: March 26, 2023

Project: No: #002

Version 1.0

Table of Contents

[1](#_Toc130765050)

[Confidential Statement 3](#_Toc130765051)

[Disclaimer 3](#_Toc130765052)

[Contact Information 3](#_Toc130765053)

[Assessment Overview 4](#_Toc130765054)

[Assessment Components 4](#_Toc130765055)

[Internal Penetration Test 4](#_Toc130765056)

[Finding Severity Ratings 5](#_Toc130765057)

[Risk Factors 5](#_Toc130765058)

[Likelihood 5](#_Toc130765059)

[Impact 5](#_Toc130765060)

[Scope 6](#_Toc130765061)

[Scope exclusion 6](#_Toc130765062)

[Client Allowances 6](#_Toc130765063)

[Executive Summary 7](#_Toc130765064)

[Attack Summary 7](#_Toc130765065)

[Security strengths 8](#_Toc130765066)

[Security Weaknesses 8](#_Toc130765067)

[Vulnerability Summary & Report Card 9](#_Toc130765068)

[Internal Penetration Test Findings 9](#_Toc130765069)

[Technical Findings 10](#_Toc130765070)

# Confidential Statement

This document exclusively belongs to Talha Security, Inc. It contains proprietary and confidential information, as such, any redistribution or duplication, as a whole or in part or in any form requires the consent of Talha Security, Inc.

However, in accordance with nondisclosure agreement and in line with the need to demonstrate compliance with penetration test requirement, Talha Security, Inc. may share the contents of this document with auditors.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. Talha Security INC. prioritized the assessment to identify the weakest security controls an attacker would exploit. Talha Security INC. recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls

# Contact Information

Metasploitable 3

|  |  |  |
| --- | --- | --- |
| NAME | TITLE | COTACT INFORMATION |
| Talha Yilmaz | CEO | Talhabugra9999@gmail.com |
|  |  |  |
|  |  |  |

Talha Security INC.

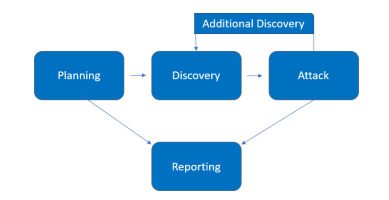
|  |  |  |
| --- | --- | --- |
| NAME | TITLE | CONTACT INFORMATION |
| Talha Yilmaz | Lead Penetration Tester | Talhabugra9999@gmail.com |
|  |  |  |
|  |  |  |

# Assessment Overview

On 3/24/23, METASPLOITABLE 3 engaged Talha Security INC. to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered, and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses



# Assessment Components

## Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| SEVERITY | CVSS V3 SCORE RANGE | DEFINITION |
| CRITICAL | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| HIGH | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| MODERATE | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| LOW | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| INFORMATIONAL | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact:

## Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

## Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

|  |  |
| --- | --- |
| ASSESSMENT | DETAILS |
| External Penetration Test | 10.0.2.10 |

## Scope exclusion

Per client request, Talha security INC. did not perform any of the following attacks during testing:

Man-in-the-middle

XSS

Social engineering

Denial of service

Phishing

## Client Allowances

METASPLOITABLE 3 provided Talha Security INC. :

Malware attacks

# Executive Summary

Talha Security INC. evaluated METASPLOTABLE 3’s internal security posture through penetration testing from March 10 to March 24. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

## Attack Summary

The following table describes how Talha Security INC. gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| STEP | ACTION | RESULT |
| 1 | Conducted a port scan of the target IP address using Nmap to identify open ports and their versions. | Open ports and their versions were discovered. |
| 2 | Using Metasploit, ProFTPD was tried to exploit. | Attempt was unsuccessful due to the /var/www not being writable |
| 3 | Drupal coder that was found on Nessus findings was tried to gain shell access. | Attempt was unsuccessful. |
| 4 | Attempt to gain access through port 22, 80, 445, 631, 3506 and 3500 with combinations of lots of modules and payloads. | Attempts were unsuccessful. |
| 5 | Attempted to gain shell access through port 6697 UnrealIRCd. | A shell access was gained. User: boba\_fett |
| 6 | Attempted to escalate privilege using 33824.c file in searchsploit with the kernel version and ubuntu version. | Attempt was unsuccessful. |
| 7 | Attempted to obtain critical informations. | /etc/passwd and ~/.bashrc were obtained. |

# Security strengths

Port 21, ProFTPD 1.3.5, was not exploitable in metasploit.

Port 22, OpenSSH 6.6.1p1, was not exploitable in metasploit.

Port 80, Apache httpd 2.4.7, was not exploitable in metasploit.

Port 445, Samba smbd 3.X - 4.X, was not exploitable in metasploit.

Port 631, CUPS 1.7, was not exploitable in metasploit.

Port 3306, MySQL, was not exploitable in metasploit.

Port 3500, WEBrick httpd 1.3.1, was not exploitable in metasploit.

Port 8080, Jetty 8.1.7.v20120910, was not exploitable in metasploit.

# Security Weaknesses

Port 6697, UnrealIRCd, was exploitable with “exploit/unix/irc/unreal\_ircd\_3281\_backdoor” module and a shell access was gained. /etc/passwd, /.bashrc etc… was accessible.

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

## Internal Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 2 | 8 | 3 | 0 |
| CRITICAL | HIGH | MODERATE | LOW | INFORMATIONAL |

|  |  |  |  |
| --- | --- | --- | --- |
| FINDING | HOSTS | SEVERITY | RECOMMENDATION |
| ProFTPD mod\_copy Information Disclosure | 10.0.2.10 | 9.8 | Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later. |
| Drupal Coder Module Deserialization RCE | 10.0.2.10 | 10  (CVSS v2.0) | Upgrade the Coder module to version 7.x-1.3 / 7.x-2.6 or later |
| Drupal Database Abstraction API SQLi | 10.0.2.10 | 7.5  (CVSS v2.0) | Upgrade to version 7/32 or later |
| SSL Medium Strength Cipher Suites Supported (SWEET32) | 10.0.2.10 | 7.5 | Reconfigure the affected application, if possible, to avoid use of medium strength ciphers. |
| Apache Multiviews Arbitrary Directory Listing | 10.0.2.10 | 5.3 | Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews. |
| IP Forwarding Enabled | 10.0.2.10 | 6.5 | On Linux, you can disable IP forwarding by doing:  echo 0 > /proc/sys/net/ipv4/ip\_forward |
| SMB Signing not required | 10.0.2.10 | 5.3 | Enforce message signing in the host's configuration. |
| SSH Weak Algorithms supported | 10.0.2.10 | 4.3  (CVSS v2.0) | Contact the vendor or consult product documentation to remove the weak ciphers. |
| SSL Certificate Cannot be trusted | 10.0.2.10 | 6.5 | Purchase or generate a proper SSL certificate for this service. |
| SSL Self-Signed Certificate | 10.0.2.10 | 6.5 | Purchase or generate a proper SSL certificate for this service. |
| TLS Version 1.0 Protocol Detection | 10.0.2.10 | 6.5 | Enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0. |
| TLS Version 1.1 Protocol Deprecated | 10.0.2.10 | 6.5 | Enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1. |
| SSH Server CBC Mode Ciphers Enabled | 10.0.2.10 | 2.6  (CVSS v2.0) | Contact the vendor or consult product documentation to disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption. |
| SSH Weak Key Exchange Algorithms Enabled | 10.0.2.10 | 3.7 | The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. |
| SSH Weak MAC Algorithms Enabled | 10.0.2.10 | 2.6  (CVSS v2.0) | Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. |

# Technical Findings

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | STATE | SERVICE | VERSION |
| 21/TCP | Open | FTP | ProFTPD 1.3.5 |
| 22/TCP | Open | SSH | OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) |
| 80/TCP | Open | HTTP | Apache httpd 2.4.7 |
| 445/TCP | Open | NETBIOS-SSN | Samba smbd 3.X - 4.X |
| 631/TCP | Open | IPP | CUPS 1.7 |
| 3306/TCP | Open | MYSQL | MySQL (unauthorized) |
| 3500/TCP | Open | HTTP | WEBrick httpd 1.3.1 |
| 6697/TCP | Open | IRC | UnrealIRCd |
| 8080/TCP | Open | HTTP | Jetty 8.1.7.v20120910 |