Duale Hochschule Baden-Württemberg
Mannheim

Pentest Report

Pentesting Project X

Studiengang Cyber Security

Verfasser:	Luka Tsipitsoudis
Matrikelnummer:	4110112
Kurs:	TINF20CS1
Abgabedatum:	18.04.2023
Betreuer:	Pr. Dr. Johannes Bauer

Unterschrift: _____

Abstract

Deutsche Version

Englische Version

Inhaltsverzeichnis

Abbildungsverzeichnis **iv**

Tabellenverzeichnis **v**

Abkürzungsverzeichnis **vi**

1 Introduction **1**
1.1 Scope 1
1.2 Severities 1
1.3 Classification 1
1.4 Effort to Fix 1

2 Management Summary **2**

3 Technical Summary **3**
3.1 Findings Overview 3
3.2 Used Tools 3

4 Findings **4**
4.1 Finding 1 - Exact SSH-Version can be determined 4
4.1.1 Finding Description 4
4.1.2 Finding Impact 4
4.1.3 Finding Cause 4
4.1.4 Finding Details 4
4.1.5 Evaluation of Results 5

5 Results **6**

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

DUT Device Under Testing

1 Introduction

1.1 Scope

Who gave the assignment? What is the Device under Test (DUT)? What have you received for the test (hardware, information, etc.)? Add email with hash sum of the mail to the report.

1.2 Severities

For each vulnerability you uncover in your testing, you typically provide: The likelihood of exploitation, taking into account how easy it is to discover and exploit The impact on the control you get once exploited Suggested remediation Suggested validation of remediation effectiveness

Low Moderate High Severe Critical

1.3 Classification

1.4 Effort to Fix

Low Moderate High

2 Management Summary

Short Summary for non technical people. what are key takeeaways and recommendations? how urgent is acting neccessary?

3 Technical Summary

summery for technical people

3.1 Findings Overview

table that contains the findings you'll describe later, sorted by severity Helps quickly triage results

3.2 Used Tools

4 Findings

4.1 Finding 1 - Exact SSH-Version can be determined

Classification: Information Disclosure **CVE:** **Severity:** Low

4.1.1 Finding Description

A nmap port scan reveils the exact version of the running SSH-Server on the Device Under Testing (DUT). The version used on the DUT is **"OpenSSH 8.4p1 Debian 5+deb11u1"** and can be accessed via port 22.

4.1.2 Finding Impact

This information can be used by an attacker to find known vulnerabilities in this specific SSH-Version to exploit the DUT.

4.1.3 Finding Cause

This finding is caused by SSH itself. There is no configuration option to hide the version of the SSH-Server. The version-banner can be found in the sshd binary.

4.1.4 Finding Details

```
1 $ nmap -sV -p 22
2 Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 14:00 CEST
3 Nmap scan report for
4 Host is up (0.00020s latency).
5 PORT STATE SERVICE VERSION
6 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
```

4.1.5 Evaluation of Results

Effort to Fix:

How do you judge the individual technical findings (severity, likelihood)? What is your suggested remediation, if there is one? How can the customer validate their remediation is effective once implemented?

5 Results