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

Tabellenverzeichnis

Abkürzungsverzeichnis

DUT Device Under Testing
AJP Apache JServ Protocol
CVE Common Vulnerabilities and Exposures

1 Introduction CHECKS NOCH ENTFERNEN

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 OpenSSH-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 OpenSSH-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 OpenSSH-Version to exploit the DUT. Possible exploitations can be found in Finding 2.

4.1.3 Finding Cause

This finding is caused by OpenSSH 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

```
$ nmap -A 172.16.0.29
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-06 09:30 CEST
Nmap scan report for 172.16.0.29
Host is up (0.00051s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
```

4.1.5 Evaluation of Results

Effort to Fix: Medium

To fix this finding the OpenSSH Binary has to be changed. By default the binary can be found at '/usr/sbin/sshd'. Change the binary with hexedit and search for the version banner. After removing the version banner restart the ssh service wit 'systemctl restart sshd.service'. Due to the fact of the risk of working on the binary itself, this finding is rated as medium effort to fix.

4.2 Finding 2 - Vulnerable OpenSSH Version

Classification:	Vulnerable Software Version	**Severity:** Medium
CVE:	CVE-2021-28041, CVE-2021-41617	

4.2.1 Finding Description

The DUT is running a vulnerable OpenSSH version (8.4p1). This version is vulnerable to the following CVEs: CVE-2021-28041, CVE-2021-41617.

4.2.2 Finding Impact

Following exploits can be used to gain access to the DUT:

CVE-2021-28041: This vulnerability enables an attacker to carry out unauthorized code execution on a target system remotely. The vulnerability stems from an error in the ssh-agent, where a remote attacker can lure the victim to connect to a server where the attacker has root access.

CVE-2021-41617: When OpenSSH is used with non default configurations privilige escalation is possible. (Check configuration)

4.2.3 Evaluation of Results

Effort to Fix: Low

Update to newer OpenSSH version. This can be done by running the following command:

```
1 $ sudo apt update
2 $ sudo apt install openssh-server
```

4.3 Finding x - Name

Information Disclosure RCE (Remote Code Execution) DoS (Denial of Service) Key reuse/sharing Weak cryptography

Classification: Vulnerable Software Version **Severity:** Medium

CVE: CVE-2023-25690, CVE-2023-27522, CVE-2006-20001, CVE-2022-36760, CVE-2022-37436

4.3.1 Finding Impact

4.3.2 Finding Details

4.3.3 Evaluation of Results

Effort to Fix: Medium

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?

4.4 Finding 4 - Vulnerable Apache Version

Classification: Vulnerable Software Version **Severity:** Medium

CVE: CVE-2023-25690, CVE-2023-27522, CVE-2006-20001, CVE-2022-36760, CVE-2022-37436

On port 80 the DUT is running a vulnerable Apache version (**"Apache 2.4.54"**). This version has multiple vulnerabilities and shouldn't be used in production. The following vulnerabilities are known from Common Vulnerabilities and Exposures (CVE) but haven't been exploited on the DUT. Some of these vulnerabilities may only be exploitable with specific configurations. Nevertheless, all of these vulnerabilities are shown to provide transparency and to show the possible impact of the vulnerabilities.

4.4.1 Finding Impact

CVE-2023-25690: When the mod_proxy configuration is enabled a HHTP smuggling attack is possible, which could bypass the access controls.

CVE-2023-27522: This vulnerability allows an attacker to send a origin header which contains special characters to the server. This could be used truncate/split the response forwarded to the client.

CVE-2006-20001: This vulnerability allows an attacker to send a specific if request to the server, which could be used to crash the process.

CVE-2022-36760: Due to an incosistent interpretation of HTTP requests of the server it could be possible for attackers to smuggle HTTP requests to the Apache JServ Protocol (AJP) server.

CVE-2022-37436: A malicious backend has the ability to terminate the response headers prematurely, leading to certain headers being integrated into the response body. Following headers which serve a security function, they will not be comprehended by the client.

4.4.2 Finding Details

```
1 $ nmap -A 172.16.0.29
2
3 Starting Nmap 7.93 ( https: //nmap.org ) at 2023-03-06 09:30 CET
4 Nmap scan report for 172.16.0.29
5 Host is up (0.00051s latency).
6
7 PORT STATE SERVICE VERSION
8 80/tep open http Apache httpd 2.4.54 ((Debian))
```

4.4.3 Evaluation of Results

Effort to Fix: Low

To fix this vulnerability the Apache Server has to be updated to a newer version. This could be done with the following command:

```
1 $ apt update && apt install apache2
```

5 Results