Offensive Security Certified Expert Exam Report

OSCE Exam Report

student@youremailaddress.com, OSID: XXXX

2020-07-25

Contents

1 Intro

The Offensive Security OSCE exam documentation contains all efforts that were conducted in order to pass the Offensive Security Certified Expert exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has the technical knowledge required to pass the qualifications for the Offensive Security Certified Expert certification. The student will be required to fill out this exam documentation fully and to include the following sections: - Methodology walkthrough and detailed outline of steps taken - Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable. - Any additional items that were not included

2 192.168.XX.200

2.1 Proof.txt

Provide the contents of proof.txt.

2.2 Vulnerable Command

Provide the command that was found to be exploitable.

2.3 Vulnerability Identification

Provide the method and code used to find the vulnerability.

2.4 PoC Code

Provide the final proof of concept code used to gain access to the server.

2.5 Steps

Provide a detailed account of your methodology in creating the exploit. The steps taken should be able to be easily followed and reproducible if necessary.

3 192.168.XX.220

3.1 Proof.txt

Provide the contents of proof.txt.

3.2 Vulnerable Command

Provide the command that was found to be exploitable.

3.3 Privilege Escalation

Provide the privilege escalation that was used to gain root on the server.

3.4 PoC Code

Provide the final proof of concept code used to gain access to the server.

3.5 Screenshots

Provide a screenshot of the id command and the contents of proof.txt.

Figure 3.1: ImgPlaceholder

3.6 Steps

Provide a detailed account of your methodology in creating the exploit. The steps taken should be able to be easily followed and reproducible if necessary.

4 192.168.XX.201

4.1 Screenshot

Screenshot requirements are detailed in the control panel.

Figure 4.1: ImgPlaceholder

4.2 Steps

Provide a detailed account of your methodology. The steps taken should be able to be easily followed and reproducible if necessary.

5 192.168.XX.240

5.1 PoC Code

Provide the final proof of concept code used to gain access to the server.

5.2 Screenshot

Screenshot requirements are detailed in the control panel.

Figure 5.1: ImgPlaceholder

5.3 Steps

Provide a detailed account of your methodology in creating the exploit. The steps taken should be able to be easily followed and reproducible if necessary.

6 Additional Items Not Mentioned in the Report

This section is placed for any additional items that were not mentioned in the overall report.