
Offensive Security Exploitation Expert Exam Report

OSEE Exam Report

student@youremailaddress.com, OSID: XXXX

2020-07-25

Contents

- 1 Intro** **1**

- 2 192.168.66.63** **2**
 - 2.1 Proof.txt 2
 - 2.2 ROP Chains with Explanations 2
 - 2.3 PoC Code 2
 - 2.4 Screenshots 2
 - 2.5 Steps 3

- 3 192.168.66.6** **4**
 - 3.1 Proof.txt 4
 - 3.2 ASM Shellcode with Explanation 4
 - 3.3 PoC Code 4
 - 3.4 Screenshots 4
 - 3.5 Steps 5

- 4 Additional Items Not Mentioned in the Report** **6**

1 Intro

The Offensive Security OSEE exam documentation contains all efforts that were conducted in order to pass the Offensive Security Exploitation 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 Exploitation 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

2 192.168.66.63

2.1 Proof.txt

Provide the contents of proof.txt

2.2 ROP Chains with Explanations

Provide the ASM ROP chains used in the exploit with a brief explanation for each gadget.

2.3 PoC Code

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

2.4 Screenshots

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



Figure 2.1: ImgPlaceholder

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.

3 192.168.66.6

3.1 Proof.txt

Provide the contents of proof.txt

3.2 ASM Shellcode with Explanation

Provide the ASM shellcode instructions used in the exploit with a brief explanation for each instruction.

3.3 PoC Code

Provide the final proof of concept code used to elevate privileges on the target.

3.4 Screenshots

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



Figure 3.1: ImgPlaceholder

3.5 Steps

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

4 Additional Items Not Mentioned in the Report

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