OFFENSIVE SECURITY

OSEE Exam Documentation

v.1.0

student@youremailaddress.com

OSID: XXXXX



Copyright © 2021 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

Table of Contents

1.0 Offensive-Security OSEE Exam Documentation 3

2.0 192.168.XX.11 (25 Points or 50 Points) 4

2.1 Proof.txt 4

2.2 Initial Exploitation 4

2.3 Read and Write Primitive 4

2.4 Code Execution 4

2.5 Sandbox Escape 4

2.6 Proof of Concept 4

2.7 Screenshots 5

3.0 192.168.XX.63 (25 or 50 Points) 6

3.1 Proof.txt 6

3.2 Race Condition 6

3.3 Kernel Memory Leak 6

3.4 Read and Write Primitive 6

3.5 Privilege Escalation 6

3.6 PoC Code 6

3.7 Screenshots 6

1.0 Offensive-Security OSEE Exam Documentation

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

2.0 192.168.XX.11 (25 Points or 50 Points)

## 2.1 Proof.txt

Provide the contents of proof.txt is complete solution is provided

## 2.2 Initial Exploitation

Explain the research performed and steps taken to perform initial exploitation with the provided CVE.

## 2.3 Read and Write Primitive

Explain the research performed and steps taken to create a read and write primitive including ASLR bypass.

## 2.4 Code Execution

Explain the research performed and steps taken to bypass all the mitigations excluding the sandbox and obtain code execution. Also include the execution of an arbitrary Win32 API if only partial solution is provided.

## 2.5 Sandbox Escape

Explain the research performed and steps taken to escape the sandbox and obtain a reverse shell.

## 2.6 Proof of Concept

Provide the code of your final exploit

## 2.7 Screenshots

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

3.0 192.168.XX.63 (25 or 50 Points)

## 3.1 Proof.txt

Provide the contents of proof.txt is complete solution is provided

## 3.2 Race Condition

Explain the research performed and steps taken to perform initial exploitation with the provided CVE.

## 3.3 Kernel Memory Leak

Explain the research performed and steps taken to perform a kernel memory leak with the provided CVE.

## 3.4 Read and Write Primitive

Explain the research performed and steps taken to create a kernel mode read and write primitive if you are submitting the full solution.

## 3.5 Privilege Escalation

Explain the research performed and steps taken to escalate your privileges to SYSTEM if you are submitting the full solution.

## 3.6 PoC Code

Provide the code of your final exploit.

## 3.7 Screenshots

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

.