EXP-312 Lab Report

v.2.0

student@youremailaddress.com

OSID: XXXXX



Copyright © 2023 Offsec 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 Offsec.

Table of Contents

1.0 Offsec EXP-312 Lab Documentation 3

1.1 Objective 3

Note that copy-pasting code from the book modules into a script may result in unintended whitespace or newlines due to formatting. 3

1.2 Extra Miles 3

1.3 Requirements 4

2.0 Exercises 5

2.1 Summary Overview 5

2.2.3 Explore which non-system applications are configured to run at startup. 5

2.3.4 Find the value of the key “CFBundleHelpBookName” in the /System/Applications/Music.app/Contents/Info.plist binary plist. (Example) 6

## 1.0 Offsec EXP-312 Lab Documentation

The following pages contains the lab exercises for the macOS Control Bypasses (EXP-312) course and should be attempted only inside the Offsec hosted lab environment. Please note that most of the attacks described in the lab guide would be illegal if attempted on machines that you do not have explicit permission to test and attack. Since the Offsec lab environment is segregated from the Internet, it is safe to perform the attacks inside the lab. Offsec does not authorize you to perform these attacks outside its own hosted lab environment and disclaims all liability or responsibility for any such actions

## 1.1 Objective

We recommend that you fully complete the exercises for each module prior to moving on to the next module. They will test your understanding of the material and build your confidence to move forward.

Depending on your existing skillset, it may take considerable time and effort to complete the exercises. Nevertheless, we encourage you to be persistent, especially with tougher exercises. Persistence is an essential trait to develop as part of the OffSec "Try Harder" mindset.

To aid in your studying the dedicated student vm contains the folder **/Users/offsec**. Inside this folder you will find any required software or code for relevant exercises for every module.

We encourage you to attempt to solve the exercises on your own before you read the solutions, as this will greatly increase your learning.

Note that copy-pasting code from the book modules into a script may result in unintended whitespace or newlines due to formatting.

## 1.2 Extra Miles

Some modules include extra mile exercises, which are more difficult and time-consuming than regular exercises. These exercises are not required to learn the material, but they will you help develop extra skills and succeed on the exam. Also note that solutions to these extra miles are not given on your student vm.

## 1.3 Requirements

The student will be required to fill out this lab report fully and to include the following sections:

* High-Level summary of assignment solutions.
* Methodology walkthrough and detailed outline of steps taken through analysis and all written code.
* Each finding with included screenshots, walkthrough, sample code or reference.
* Screenshots of the final working exploit against your target.

2.0 Exercises

## 2.1 Summary Overview

A brief description of the assignments that were solved, including the overall exploitation / development steps.

E.g.: Exploring the MacOS file system to know the content of relevant bundles and folders.

2.2 High-Level OS Architecture: The dyld Shared Cache: (Example Exercise)

## 2.2.3 Explore which non-system applications are configured to run at startup.

First, we need to check the relevant launchd folders:



Then, we can check the content of launchd files:

We can find that there are two apps setup to launch. Those are:

## 2.3.4 Find the value of the key “CFBundleHelpBookName” in the /System/Applications/Music.app/Contents/Info.plist binary plist. (Example)

The plist is binary so we need to convert it with plutil. Then we can either search the full output for the key or simply grep for it.