OFFENSIVE SECURITY

OSWP 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 OSWP Exam Documentation 3

2.0 Reconnaissance 4

2.1 Steps 4

2.2 Lab Informations 4

3.0 STAGE 1 5

3.1 Wireless Network Key 5

3.2 Screenshots 5

3.3 Steps 5

4.0 STAGE 2 6

4.1 Wireless Network Key 6

4.2 Screenshots 6

4.3 Steps 6

5.0 STAGE 3 7

5.1 Wireless Network Key 7

5.2 Screenshots 7

5.3 Steps 7

6.0 Additional Items Not Mentioned in the Report 8

## 1.0 Offensive-Security OSWP Exam Documentation

The Offensive Security OSWP exam documentation contains all efforts that were conducted in order to pass the Offensive Security Wireless Professional 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 Wireless Professional certification.

You are 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, and sample commands
* Any additional items that were not included

## 2.0 Reconnaissance

## 2.1 Steps

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

## 2.2 Lab Informations

**STAGE 1 :**

* BSSID = <BSSID>
* Channel = <Channel>
* Enc = <WEP/WPA>

**STAGE 2 :**

* BSSID = <BSSID>
* Channel = <Channel>
* Enc = <WEP/WPA>

**STAGE 3 :**

* BSSID = <BSSID>
* Channel = <Channel>
* Enc : <WEP/WPA>

**Alfa Card MAC address :** <MAC Address>

# 3.0 STAGE 1

* BSSID = <BSSID>
* Channel = <Channel>
* Enc = <WEP/WPA>

## 3.1 Wireless Network Key

Provide the contents of the “STAGE 1” wireless network key.

## 3.2 Screenshots

Provide at least one screenshot of the successfully cracked “STAGE 1” wireless network key.

## 3.3 Steps

Provide a detailed account of your methodology in obtaining the “STAGE 1” wireless network key. The steps taken should be able to be easily followed and reproducible if necessary.

# 4.0 STAGE 2

* BSSID = <BSSID>
* Channel = <Channel>
* Enc = <WEP/WPA>

## 4.1 Wireless Network Key

Provide the contents of the “STAGE 2” wireless network key.

## 4.2 Screenshots

Provide at least one screenshot of the successfully cracked “STAGE 2” wireless network key.

## 4.3 Steps

Provide a detailed account of your methodology in obtaining the “STAGE 2” wireless network key. The steps taken should be able to be easily followed and reproducible if necessary.

# 5.0 STAGE 3

* BSSID = <BSSID>
* Channel = <Channel>
* Enc = <WEP/WPA>

## 5.1 Wireless Network Key

Provide the contents of the “STAGE 3” wireless network key.

## 5.2 Screenshots

Provide at least one screenshot of the successfully cracked “STAGE 3” wireless network key.

## 5.3 Steps

Provide a detailed account of your methodology in obtaining the “STAGE 3” wireless network key. The steps taken should be able to be easily followed and reproducible if necessary.

# 6.0 Additional Items Not Mentioned in the Report

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