



OffSec Wireless Professional

Exam Report

OSID: OS-XXXXX
student@example.com

September 30, 2025

v2.0

Table of Contents

1 OffSec Wireless Professional Exam Report	3
1.1 Requirements	3
2 Access Point Y	4
2.1 Proof	4
2.2 Screenshots	4
2.3 Steps	4
3 Access Point X	5
3.1 Proof	5
3.2 Screenshots	5
3.3 Steps	5
4 Additional Items Not Mentioned in the Report	6

1 OffSec Wireless Professional Exam Report

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

1.1 Requirements

The student will be required to fill out this penetration testing report 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 Access Point Y

While monitoring the wifi activity in the area, I discovered Access Point Y. Further enumeration I discovered that Access Point Y was transmitting on channel X and using XYZ as its security algorithm. I proceeded by collecting information by utilizing the XYZ attack, till there was enough information to crack the key using the 123 cracking tool.

2.1 Proof

The "Access Point 2" wireless network key: **DE:AD:CA:FE:BA:BE:99:77:55:33:11:88:66** The "Access Point Y" proof.txt: **b78066a8ec18b4182da1209471a6ce95**

2.2 Screenshots



Figure 1 - Cracked wireless key

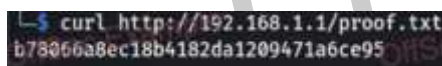
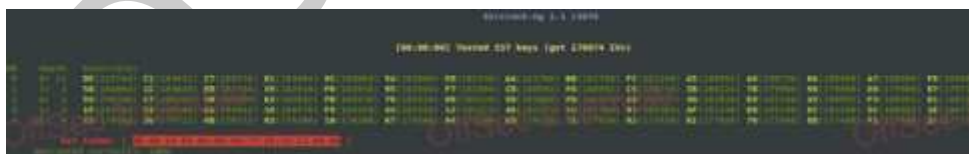


Figure 2 - Cracked wireless key

2.3 Steps

1. Placed interface in monitor mode. *Command and/or screenshots*
2. Next Step *Command and/or screenshots*
3. Crack the key using the 123 cracking tool.



3 Access Point X

TODO A brief description of the attack chain with machine names, including the depth of compromise should be included here.

3.1 Proof

TODO Provide the contents of the "Access Point X" wireless network key.

3.2 Screenshots

TODO Provide at least one screenshot of the successfully cracked "Access Point X" wireless network key and a screenshot of proof.txt.

3.3 Steps

TODO Provide a detailed account of your methodology in obtaining the "Access Point X" wireless network key. **The steps taken should be able to be easily followed and reproducible if necessary.**

OS-X-XXXXXX

4 Additional Items Not Mentioned in the Report

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

OS-X-XXXXXX

End of Report

*This report was rendered
by [SysReptor](#) with*



OS-X-XXXXXX