**OffSec Certified Professional (OSCP)**

**Exam Report**

your.email@example.com

**OSID: [YOUR-OSID-HERE]**

A blue and purple circle with lines in it

Description automatically generated

Copyright © 2024 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

[OffSec Certified Professional Exam Report 3](#_Toc197265442)

[1.1 Introduction 3](#_Toc197265443)

[1.2 Objectives 3](#_Toc197265444)

[1.3 Requirements 3](#_Toc197265445)

[2. High-Level Summary 3](#_Toc197265446)

[2.1 Recommendations 3](#_Toc197265447)

[3. Methodologies 4](#_Toc197265448)

[3.1 Information Gathering 4](#_Toc197265449)

[3.2 Service Enumeration 4](#_Toc197265450)

[3.3 Penetration 4](#_Toc197265451)

[4. Active Directory Set 5](#_Toc197265452)

[4.1 [IP-ADDRESS-OF-AD-TARGET-1-HERE] 5](#_Toc197265453)

[4.1.1 Nmap scan 5](#_Toc197265454)

[4.1.2 Privilege escalation 5](#_Toc197265455)

[4.2 [IP-ADDRESS-OF-AD-TARGET-2-HERE] 5](#_Toc197265456)

[4.2.1 Nmap scan 5](#_Toc197265457)

[4.2.2 Initial foothold 5](#_Toc197265458)

[4.2.3 Privilege escalation 5](#_Toc197265459)

[4.3 [IP-ADDRESS-OF-AD-TARGET-3-HERE] 5](#_Toc197265460)

[4.3.1 Nmap scan 5](#_Toc197265461)

[4.3.2 Initial foothold 5](#_Toc197265462)

[4.3.3 Privilege escalation 5](#_Toc197265463)

[5. Standalone machines 5](#_Toc197265464)

[5.1 [IP-ADDRESS-OF-STANDALONE-TARGET-1-HERE] 5](#_Toc197265465)

[5.1.1 Nmap scan 5](#_Toc197265466)

[5.1.2 Initial foothold 5](#_Toc197265467)

[5.1.3 Privilege escalation 5](#_Toc197265468)

# OffSec Certified Professional Exam Report

## Introduction

The OffSec Certified Professional exam report contains all efforts that were conducted in order to pass the OffSec Certified Professional exam. This report should contain all items that were used to pass the overall exam, and it 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 OffSec Certified Professional.

## Objectives

The objective of this assessment is to perform an internal penetration test against the OffSec Lab and Exam network. The student is tasked with following a methodical approach to obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you in the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

## Requirements

The student will be required 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 proof.txt if applicable.
* Any additional items that were not included.

# High-Level Summary

Successful exploitation resulted in the compromise of the Active Directory environment, with all three associated proof files retrieved. Full administrative compromise, yielding both local (user) and proof (root) files, was achieved on standalone targets [IP-OF-FULLY-COMPROMISED-STANDALONE-1] and [IP-OF-FULLY-COMPROMISED-STANDALONE-2]. On the final standalone target, [IP-OF-USER-ONLY-STANDALONE], user-level access was obtained, allowing for the retrieval of the local proof file only; administrative access was not achieved on this host during the engagement.

## Recommendations

To address the vulnerabilities exploited during this assessment, the following key actions are recommended:

* **Patch Management:** Implement timely and consistent patching for operating systems and third-party applications.
* **[INSERT-SPECIFIC-RECOMMENDATIONS-BASED-ON-FINDINGS]**

Implementing these recommendations will significantly reduce the attack surface and mitigate the risks identified in this report.

# Methodologies

Student utilized a widely adopted approach to performing penetration testing that is effective in testing how well the OffSec Exam environment is secure. Below is a breakout of how Student 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, Student was tasked with exploiting exam network. The specific IP addresses were:

**Exam Network:**

* AD Network: [LIST-ALL-AD-TARGET-IPS-HERE]
* Standalone machines: [LIST-ALL-STANDALONE-TARGET-IPS-HERE]

## Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors in a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

## Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, Student was able to successfully gain access to all available machines.

# Active Directory Set

## [IP-ADDRESS-OF-AD-TARGET-1-HERE]

### Nmap scan

### Privilege escalation

## [IP-ADDRESS-OF-AD-TARGET-2-HERE]

### Nmap scan

### Initial foothold

### Privilege escalation

## [IP-ADDRESS-OF-AD-TARGET-3-HERE]

### Nmap scan

### Initial foothold

### Privilege escalation

# Standalone machines

## [IP-ADDRESS-OF-STANDALONE-TARGET-1-HERE]

### Nmap scan

### Initial foothold

### Privilege escalation