OffSec Certified Professional

Exam Report

v.2.0

student@youremailaddress.com

OSID: XXXXX

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

[1 OffSec Certified Professional Exam Report 4](#_Toc190077243)

[1.1 Introduction 4](#_Toc190077244)

[1.2 Objective 4](#_Toc190077245)

[1.3 Requirements 4](#_Toc190077246)

[2 High-Level Summary 4](#_Toc190077247)

[2.1 Recommendations 4](#_Toc190077248)

[3 Methodologies 4](#_Toc190077249)

[3.1 Information Gathering 4](#_Toc190077250)

[3.2 Service Enumeration 4](#_Toc190077251)

[3.3 Penetration 4](#_Toc190077252)

[3.4 Maintaining Access 4](#_Toc190077253)

[3.5 House Cleaning 4](#_Toc190077254)

[4 Independent Challenges 5](#_Toc190077255)

[4.1 Target #1 – 5](#_Toc190077256)

[4.1.1 Initial Access – 5](#_Toc190077257)

[4.1.2 Service Enumeration 5](#_Toc190077258)

[4.1.3 Initial Access – 5](#_Toc190077259)

[4.1.4 Privilege Escalation - 5](#_Toc190077260)

[4.1.5 Post Exploitation 5](#_Toc190077261)

[4.2 Target #2 – 5](#_Toc190077262)

[4.2.1 Initial Access – 5](#_Toc190077263)

[4.2.2 Service Enumeration 5](#_Toc190077264)

[4.2.3 Initial Access – 5](#_Toc190077265)

[4.2.4 Privilege Escalation - 5](#_Toc190077266)

[4.2.5 Post Exploitation 5](#_Toc190077267)

[4.3 Target #3 – 6](#_Toc190077268)

[4.3.1 Initial Access – 6](#_Toc190077269)

[4.3.2 Service Enumeration 6](#_Toc190077270)

[4.3.3 Initial Access – 6](#_Toc190077271)

[4.3.4 Privilege Escalation - 6](#_Toc190077272)

[4.3.5 Post Exploitation 6](#_Toc190077273)

[5 Active Directory Set 7](#_Toc190077274)

[5.1 Machine 1 – 7](#_Toc190077275)

[5.1.1 Initial Access – 7](#_Toc190077276)

[5.1.2 Privilege Escalation – 7](#_Toc190077277)

[5.1.3 Post-Exploitation 7](#_Toc190077278)

[5.2 Machine 2– 7](#_Toc190077279)

[5.2.1 Initial Access – 7](#_Toc190077280)

[5.2.2 Post-Exploitation 7](#_Toc190077281)

[5.3 DC – 7](#_Toc190077282)

[5.3.1 Initial Access – 7](#_Toc190077283)

# OffSec Certified Professional Exam Report

## Introduction

## Objective

## Requirements

# High-Level Summary

## Recommendations

# Methodologies

## Information Gathering

## Service Enumeration

## Penetration

## Maintaining Access

## House Cleaning

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Independent ChallengesTarget #1 –Initial Access –Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  |  |  Initial Access – **Local.txt value:** Privilege Escalation -Post Exploitation **Proof.txt value:** Target #2 –Initial Access –Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  |  |  Initial Access – **Local.txt value:** Privilege Escalation -Post Exploitation **Proof.txt value:** Target #3 –Initial Access –Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  |  |  Initial Access – **Local.txt value:** Privilege Escalation -Post Exploitation **Proof.txt value:** |  |
| Active Directory Set **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  |  | |  |  | |  |  |  Machine 1 –Initial Access –Privilege Escalation –Post-Exploitation **System Proof screenshot:** Machine 2–Initial Access –Post-Exploitation **Local Proof Screenshot:** DC –Initial Access – **System Proof Screenshot:** | |