OffSec Certified Professional Exam Report

OSCP Exam Report

CANDIDATE	hacker@cia.gov
OSID	OS-12345678
DATE	2026-06-13

Table of Contents

OffSec Certified Professional Exam Report

Introduction

This report documents all work the student performed in pursuit of passing the OffSec Certified Professional exam. It records every step taken during the engagement, and grading evaluates both the correctness and the completeness with which the exam objectives are addressed. The intent of the report is to establish that the student has both a comprehensive understanding of penetration-testing methodology and the technical proficiency required to earn the OSCP certification.

Objective

The goal of this assessment is to conduct an internal penetration test against the OffSec exam network. The student must follow a methodical approach to reach each of the engagement's objectives. The exam is meant to mirror a real penetration test in its entirety, from initial reconnaissance through to the final report.

Requirements

The student must complete the report in full, including the following sections:

- A non-technical high-level summary and recommendations
- A methodology walkthrough with a detailed outline of every step taken
- Each finding, with proof-of-concept code and screenshots of each proof (`local.txt`, `proof.txt`)
- Any additional items not covered above

High-Level Summary (Non-Technical)

The student was tasked with conducting an internal penetration test against the OffSec exam environment. An internal penetration test is a focused attack against systems on a private network. The student's goal was to map the network, enumerate live systems, exploit weaknesses, and document the findings for OffSec.

Throughout the engagement, the student identified a number of significant vulnerabilities on the in-scope systems. By chaining these together, the student was able to obtain administrative access on multiple hosts.

See the Proof and Local Contents section for the complete proof table.

Recommendations

The student recommends remediating each vulnerability identified during the engagement so that a future attacker cannot abuse the same weaknesses.

Methodologies

The student followed a widely adopted penetration-testing methodology, well-suited to evaluating the security posture of the OffSec exam environment. The sections that follow describe how the student identified and exploited each in-scope system, along with every individual vulnerability discovered.

Information Gathering

The information-gathering phase establishes the scope of the engagement. For this exam, the student was tasked with compromising the hosts on the exam network. The in-scope addresses were:

Exam network:

```
192.168.X.10
192.168.X.11
192.168.X.12
192.168.X.206
172.16.X.201
172.16.X.200
```

Service Enumeration

The service enumeration phase gathers information about which services are alive on each in-scope host. This information drives the selection of initial access vectors and is invaluable to the attacker.

IP (Hostname)	Open ports
192.168.X.10	T:21-22,80,5432
192.168.X.11	T:80,135,139,443,445,3389,5357,5432,5985
192.168.X.12	T:21,80,135,139,443,445,3306,5040,5985,9221
192.168.X.206 (WS01)	T:80,135,139,443,445,3306,3389,5040,5985
172.16.X.201 (SRV01)	T:135,139,445,1433,3389,5985
172.16.X.200 (DC01)	T:53,80,88,135,139,389,445,464,593,636,3268-3269,3389,5985

Note: the "Open ports" column uses nmap port spec notation

Each target was scanned with `nmap` using a command such as the following:

```
nmap -sC -sV --min-rate=2000 -oN scan.nmap -p- 192.168.X.10
```

Penetration

The penetration phase focuses on exploiting the vulnerabilities identified during enumeration in order to gain access to each in-scope system. During this engagement, the student successfully obtained access to every required host across both the standalone challenges and the Active Directory set.

Maintaining Access

Maintaining access ensures the attacker can return to a compromised system without re-running the initial exploit. Common approaches include planting backdoors, creating persistent accounts, or installing implants. For this exam, the student deployed rootkits on all compromised targets to enable persistence after system reboots.

House Cleaning

House cleaning removes the artifacts of the engagement from compromised systems. Tools that were uploaded, accounts that were created, and configuration changes that were made for exploitation purposes are reverted, returning the environment to its pre-engagement state.

Standalone Challenges

Target #1 - 192.168.X.10

Service Enumeration

Output from `nmap` and any other service-specific recon tooling goes here.

Initial Access

Vulnerability exploited: A one-line description of the vulnerability used to obtain initial access on the target.

Vulnerability description:

A paragraph explaining the vulnerability.

Severity: Critical, High, Medium, or Low.

Vulnerability fix:

Remediation steps go here.

Proof of Concept:

Commands executed and their output go here.

Screenshot showing `whoami`, hostname, IP, and `local.txt` content:

Privilege Escalation

Vulnerability exploited: A one-line description of the vulnerability used to escalate from the initial access user to a privileged user.

Vulnerability description:

A paragraph explaining the vulnerability.

Severity: Critical, High, Medium, or Low.

Vulnerability fix:

Remediation steps go here.

Proof of Concept:

Commands executed and their output go here.

Screenshot showing `whoami`, hostname, IP, and `proof.txt` content:

Target #2 - 192.168.X.11

Service Enumeration

Initial Access

Privilege Escalation

Target #3 - 192.168.X.12

Service Enumeration

Initial Access

Privilege Escalation

Active Directory Set

WS01 - 192.168.X.206

Service Enumeration

Initial Access

Privilege Escalation

SRV01 - 172.16.X.201

Service Enumeration

Initial Access

Privilege Escalation

DC01 - 172.16.X.200

Service Enumeration

Initial Access

Privilege Escalation

Additional Items

Appendix - Proof and Local Contents

IP (Hostname)	`local.txt`	`proof.txt`
192.168.X.10	`00000000000000000000000000000000`	`aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa`
192.168.X.11	`11111111111111111111111111111111`	`bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb`
192.168.X.12	`22222222222222222222222222222222`	`cccccccccccccccccccccccccccccccc`
192.168.X.206 (WS01)	n/a	`dddddddddddddddddddddddddddddddd`
172.16.X.201 (SRV01)	n/a	`eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee`
172.16.X.200 (DC01)	n/a	`ffffffffffffffffffffffffffffffff`