Offensive Security

OSCP Lab Report

OSID: XXXXX
student@example.com

v1.0

Table of Contents

1 Offensive Security OSCP Lab Penetration Test Report

1.1 Objective

John Doe (XXXXX) was tasked with performing an internal penetration test towards Offensive Security Labs. 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 lab systems – the THINC.local domain. John Doe's (XXXXX) overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security's network. When performing the attacks, John Doe (XXXXX) was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, John Doe (XXXXX) had administrative level access to multiple systems. All systems were successfully exploited and access granted.

TODO Adapt summary as required

1.2 Lab Network

Offensive Security Complete Guide machines (alpha and beta) may not be included in your lab report, they are for demonstration purposes only.

For more information regarding the Bonus Points requirements, please visit the following URL: *https://help.offensive-security.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide*

TODO Adapt as required

1.3 Identified Vulnerabilities

In the course of this penetration test **1 Info** vulnerabilities were identified:

Target Name	IP	CVSS	Page
Target #1	TODO IP Address	0.0	4

2 Lab Network

Target #1 (TODO IP Address)

Score:	0.0 (Info)
Vector:	N/A

Initial Access

TODO Describe initial access

Privilege Escalation

TODO Describe privilege escalation

Post-Exploitation

TODO Describe Post Exploitation

3 Course Exercises

TODO a.b.c.d Exercise (e.g. "2.4.3.4 - Finding Files in Kali Linux")

TODO Adapt as required