Offensive Security Certified Professional Lab Report

PWK Lab Report

student@youremailaddress.com, OSID: XXXX

2021-05-19

Contents

1 Offensive Security OSCP Lab Report **1**

1.1 Introduction 1

1.2 Objective 1

1.3 Requirements 1

2 High-Level Summary **2**

2.1 Recommendations 2

3 Methodologies **3**

3.1 Information Gathering 3

3.2 Service Enumeration 3

3.3 Penetration 4

3.4 Maintaining Access 4

3.5 House Cleaning 5

4 PWK Course Exercisese **6**

1 Offensive Security OSCP Lab Report

1.1 Introduction

The Offensive Security Lab penetration test report should contain all the steps taken to successfully compromise machines both in the exam and lab environments. Accompanying data used in both environments should also be included, such as PoCs, custom exploit code, and so on. Please note that this report will be graded from a standpoint of correctness and completeness. 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 required to successfully achieve the Offensive Security Certified Professional (OSCP) certification.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Offensive Security Lab network. The student is tasked with following methodical approach in 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. A sample page has been included in this document that should help you determine what is expected of you from a reporting standpoint. Please use the sample report as a guide to get you through the reporting requirement of the course.

1.3 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 as deemed necesarry

2 High-Level Summary

OS-XXXXX was tasked with performing an internal penetration test in the Offensive Security Labs and Exam network. An internal penetration test is a simulated attack against internally connected systems.

The focus of this test is to perform attacks, similar to those of a malicious entity, and attempt to infiltrate Offensive Security's internal lab systems – the THINC.local domain, and the exam network. OSXXXXX's overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

While conducting the internal penetration test, there were several alarming vulnerabilities that were identified within Offensive Security's network. For example, OS-XXXXX was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During testing, OS-XXXXX had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- Target #1 – Obtained a low-privilege shell via the vulnerable web application called 'KikChat'. Once in, access was leveraged to escalate to 'root' using the 'getsystem' command in Meterpreter.

2.1 Recommendations

OS-XXXXX recommends patching the vulnerabilities identified during the penetration test 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 in order to mitigate additional vulnerabilities that may be discovered at a later date.

3 Methodologies

OS-XXXXX utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Labs and Exam environments are secure. Below is a summary of how OS-XXXXX was able to identify and exploit a number of systms.

3.1 Information Gathering

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

Lab Network

- 192.168.
- 192.168.
- 192.168.
- 192.168.
- 192.168.

3.2 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 into 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.

Server IP Address	Ports Open
192.168.x.x	**TCP**: 1433,3389 **UDP**: 1434,161

3.3 Penetration

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

3.3.1

System Vulnerable:

Vulnerability Explanation:

Privilege Escalation Vulnerability:

Vulnerability Fix:

Severity:

Information Gathering:

Proof of Concept Code: (link to exploitdb or code)

Confirming RCE:

Getting Low-Privilege Shell:

Privilege Escalation:

Local.txt File:

Proof.txt File:

3.4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system 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 (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

3.5 House Cleaning

The house-cleaning portion of the assessment ensures that remnants of the penetration test are removed. Often times, fragments of tools or user accounts are left on an organization's computer, which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is paramount importance.

After the objectives on both the lab network and exam network were successfully completed, OS-XXXXX removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from any of the systems.

4 PWK Course Exercisese