Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@youremailaddress.com, OSID: XXXX

2023-04-06

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report 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 Offensive Security Certified Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Offensive Security Exam 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. An example page has already been created for you at 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.

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 that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Offensive Security Exam. 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 exam systems - the THINC.local domain. My 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 When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I 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:

- 192.168.xx.xx (hostname) - Name of initial exploit
- 192.168.xx.xx (hostname) - Name of initial exploit
- 192.168.xx.xx (hostname) - Name of initial exploit
- 192.168.xx.xx (hostname) - Name of initial exploit
- 192.168.xx.xx (hostname) - BOF

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing 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 to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

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, I was tasked with exploiting the exam network. The specific IP addresses were:

Exam 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.

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.

3.4 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 portions of the assessment ensures that remnants of the penetration test are removed. Often 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 important.

After collecting trophies from the exam network was completed, I 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 the system.

4 Independent Challenges

4.1 Target #1 - 192.168.x.x

4.1.1 Service Enumeration

Server IP Address	Ports Open
192.168.x.x	**TCP**: 21,1433,3389 **UDP**: 1434,161

Nmap Scan Results:

Upon manual enumeration of the available FTP service, John noticed it was running an outdated version 2.3.4 that is prone to the remote buffer overflow vulnerability.

4.1.2 Initial Access - Buffer Overflow

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

4.1.3 Privilege Escalation - MySQL Injection

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code:

4.1.4 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

4.2 Target #2 - 192.168.x.x

4.2.1 Service Enumeration

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

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

4.2.2 Initial Access -

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

4.2.3 Privilege Escalation -

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code:

4.2.4 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

4.3 Target #3 - 192.168.x.x

4.3.1 Service Enumeration

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

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

4.3.2 Initial Access -

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

4.3.3 Privilege Escalation -

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code:

4.3.4 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

5 Active Directory Set

5.1 Service Enumeration

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

Nmap Scan Results:

5.2 Hostname1: 192.168.x.x

5.2.1 Initial Access -

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

5.2.2 Privilege Escalation -

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code:

5.2.3 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

5.3 Hostname2: 192.168.x.x

5.3.1 Initial Access -

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

5.3.2 Privilege Escalation -

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code:

5.3.3 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

5.4 Hostname3: 192.168.x.x

5.4.1 Initial Access -

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Proof of Concept Code:

Local.txt Proof Screenshot

Local.txt Contents

5.4.2 Privilege Escalation -

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Steps to reproduce the attack:

Exploit Code: Please see Appendix 1 for the complete Windows Buffer Overflow code.

5.4.3 Post-Exploitation

Proof Screenshot Here:

Proof.txt Contents:

6 Additional Items

6.1 Appendix - Proof and Local Contents:

IP (Hostname)	Local.txt Contents	Proof.txt Contents
192.168.x.x	hash_here	hash_here
192.168.x.x	hash_here	hash_here
192.168.x.x	hash_here	hash_here
192.168.x.x	hash_here	hash_here
192.168.x.x	hash_here	hash_here
192.168.x.x	hash_here	hash_here

6.2 Appendix - Metasploit/Meterpreter Usage

For the exam, I used my Metasploit/Meterpreter allowance on the following machine: `192.168.x.x`

6.3 Appendix - Completed Buffer Overflow Code

```
from pwn import *

io = remote('domain.com', 4242)
io.sendline('Sample code highlighting test.')
io.recvline()
# 'This seems to work!\n'
```