**OFFENSIVE SECURITY**

Penetration Test Report for   
**OSCP** Exam

Date

Email

OSID: XXXXX



Copyright © 2021 Offensive Security 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 Offensive Security.

**Table of Contents**

**1.0 Offensive Security Exam Penetration Test Report 4**

*1.1 Introduction* 4

*1.2 Objective* 4

*1.3 Requirements* 4

**2.0 High-Level Summary 5**

*2.1 Recommendations* 5

*2.2 Risk exposure over time* 5

**3.0 Report - Methodologies 6**

*3.1 Information Gathering* 6

*3.2 Report - Penetration* 6

***3.3 System: X.X.X.X* 7**

*3.3.1 Service Enumeration* 7

*3.3.2 FootHold* 8

*3.3.3 Getting Reverse Shell* X

*3.3.4 Getting User: local.txt*  X

*3.3.5 Privilege Escalation* X

*3.3.6 Getting Root: proof.txt* X

*3.3.7 Vulnerability Fix and Severity* X

*3.3.8 Proof of Concept Code* X

***3.4 System: X.X.X.X* X**

*3.4.1 Service Enumeration* X

*3.4.2 FootHold* X

*3.4.3 Getting Reverse Shell* X

*3.4.4 Getting User: local.txt*  X

*3.4.5 Privilege Escalation* X

*3.4.6 Getting Root: proof.txt* X

*3.4.7 Vulnerability Fix and Severity* X

*3.4.8 Proof of Concept Code* X

***3.5 System: X.X.X.X* X**

*3.5.1 Service Enumeration* X

*3.5.2 FootHold* X

*3.5.3 Getting Reverse Shell* X

*3.5.4 Getting User: local.txt*  X

*3.5.5 Privilege Escalation* X

*3.5.6 Getting Root: proof.txt* X

*3.5.7 Vulnerability Fix and Severity* X

*3.5.8 Proof of Concept Code* X

***3.6 System: X.X.X.X* X**

*3.6.1 Service Enumeration* X

*3.6.2 FootHold* X

*3.6.3 Getting Reverse Shell* X

*3.6.4 Getting Root: proof.txt*  X

*3.6.5 Vulnerability Fix and Severity* X

*3.6.6 Proof of Concept Code* X

***3.7 System: X.X.X.X* X**

*3.7.1 Service Enumeration* X

*3.7.2 Explanation of the development process* X

*3.7.3 Getting Reverse Shell and Root: proof.txt* X

*3.7.4 Completed Buffer Overflow Code* X

*3.8 Maintaining Access* X

*3.9 House Cleaning* X

**4.0 Additionals Item X**

# 1.0 Offensive Security Exam Penetration Test 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 a 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

# 

# 2.0 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 all 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. This is the list of systems we had:

* X.X.X.X
* X.X.X.X
* X.X.X.X
* X.X.X.X
* X.X.X.X

**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.

**2.2 Risk Exposure over Time**

The overall risk identified following the penetration test is very high. Due to the severity of some vulnerabilities, immediate action is desirable. It is reasonable to believe that a malicious attacker would be able to successfully carry out an attack against all this systems.

**3.0 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**

* X.X.X.X
* X.X.X.X
* X.X.X.X
* X.X.X.X
* X.X.X.X

## **3.2 Report - Penetration**

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, OS-XXXXX was able to successfully gain access to **X** out of the 5 systems.

## 3.**3** **System IP: X.X.X.X**

#### 3.3.1 Service Enumeration

|  |  |
| --- | --- |
| 80 | http |
| 443 | https |
| 22456 | Service 1 example |

**Nmap Scan Results:**

*Insert the Nmap screen.*

**3.3.2 FootHold:**

*Insert the foothold part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.3.3 Getting Reverse shell:**

*Insert the getting reverse shell part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.3.4 Getting User: Local.txt:**

*Insert the User screen with local.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

Local.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.3.5 Privilege Escalation:**

*Insert the privilege escalation part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.3.6 Getting Root: proof.txt:**

*Insert the Root screen with proof.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

proof.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.3.7 Vulnerability Fix and Severity:**

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

**3.3.8 Proof of Concept Code:**

*space to insert links of any exploits used, vulnerabilities and code insertion of any modified exploits.*

## 3.**4** **System IP: X.X.X.X**

#### 3.**4**.1 Service Enumeration

|  |  |
| --- | --- |
| 80 | http |
| 443 | https |
| 22456 | Service 1 example |

**Nmap Scan Results:**

*Insert the Nmap screen.*

**3.4.2 FootHold:**

*Insert the foothold part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.4.3 Getting Reverse shell:**

*Insert the getting reverse shell part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.4.4 Getting User: Local.txt:**

*Insert the User screen with local.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

Local.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.4.5 Privilege Escalation:**

*Insert the privilege escalation part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.4.6 Getting Root: proof.txt:**

*Insert the Root screen with proof.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

proof.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.4.7 Vulnerability Fix and Severity:**

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

**3.4.8 Proof of Concept Code:**

*space to insert links of any exploits used, vulnerabilities and code insertion of any modified exploits.*

## 3.**5** **System IP: X.X.X.X**

#### 3.**5**.1 Service Enumeration

|  |  |
| --- | --- |
| 80 | http |
| 443 | https |
| 22456 | Service 1 example |

**Nmap Scan Results:**

*Insert the Nmap screen.*

**3.5.2 FootHold:**

*Insert the foothold part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.5.3 Getting Reverse shell:**

*Insert the getting reverse shell part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.5.4 Getting User: Local.txt:**

*Insert the User screen with local.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

Local.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.5.5 Privilege Escalation:**

*Insert the privilege escalation part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.5.6 Getting Root: proof.txt:**

*Insert the Root screen with proof.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

proof.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.5.7 Vulnerability Fix and Severity:**

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

**3.5.8 Proof of Concept Code:**

*space to insert links of any exploits used, vulnerabilities and code insertion of any modified exploits.*

## 3.**6** **System IP: X.X.X.X**

#### 3.**6**.1 Service Enumeration

|  |  |
| --- | --- |
| 80 | http |
| 443 | https |
| 22456 | Service 1 example |

**Nmap Scan Results:**

*Insert the Nmap screen.*

**3.6.2 FootHold:**

*Insert the foothold part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.6.3 Getting Reverse shell:**

*Insert the getting reverse shell part.*

*Command:*

|  |
| --- |
| Command x 1 |

**3.6.4 Getting Root: proof.txt:**

*Insert the Root screen with proof.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

proof.txt: XXXXXXXXXXXXXXXXXXXXXX

**3.6.5 Vulnerability Fix and Severity:**

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

----------------------------------------------------

*space for explanation of vulnerabilities and fixes*

*Severity: Critical*

**3.6.6 Proof of Concept Code:**

*space to insert links of any exploits used, vulnerabilities and code insertion of any modified exploits.*

## 3.**7** **System IP: X.X.X.X**

#### 3.**7**.1 Service Enumeration

|  |  |
| --- | --- |
| 80 | http |
| 443 | https |
| 22456 | Service 1 example |

**Nmap Scan Results:**

*Insert the Nmap screen.*

#### 3.**7**.**2 Explanation of the development process**

*Provide written detailed documentation of the exploit development process. Explain all the steps taken between reviewing the given proof of concept and finalizing your exploit code.*

*Include your process for finding a valid return address, your discovery of bad characters, the full final exploit code used and any MSFvenom command(s) you have used to generate shellcode.*

*Your report must contain informative screenshots of the debugger for each major step taken.*

*Command:*

|  |
| --- |
| xxxxxxx |

**3.7.2 Getting Reverse shell and root: proof.txt**

*Insert the Root screen with proof.txt / ifconfig/ipconfig/ip address / hostname / id/whoami.*

*proof.txt: XXXXXXXXXXXXXXXXXXXXXX*

**3.7.3 Completed Buffer Overflow Code**

|  |
| --- |
| #!/usr/bin/python  xxxxxx |

## 3.3 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.

## 3.4 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, the student 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.

# 4.0 Additional Items

##### Appendix 1 - Proof and Local Contents:

|  |  |  |
| --- | --- | --- |
| **IP** | **Local.txt Contents** | **Proof.txt Contents** |
| X.X.X.X |  |  |
| X.X.X.X |  |  |
| X.X.X.X |  |  |
| X.X.X.X |  |  |
| X.X.X.X |  |  |

##### 

##### 

This Penetration Test report was developed Month, day, year