Security Assessment Report

Student: Firstname Lastname

**Table of Contents**

[1.0 Security Assessment Report 3](#_Toc65396797)

[1.1 Introduction 3](#_Toc65396798)

[1.2 Objective 3](#_Toc65396799)

[1.3 Requirements 3](#_Toc65396800)

[2.0 High-Level Summary 4](#_Toc65396801)

[2.1 Recommendations 5](#_Toc65396802)

[3.0 Methodologies 5](#_Toc65396803)

[3.1 Information Gathering 5](#_Toc65396804)

[3.2 Penetration 6](#_Toc65396805)

[System IP: 192.168.192.231 6](#_Toc65396806)

[Service Enumeration 6](#_Toc65396807)

[Privilege Escalation 6](#_Toc65396808)

[System IP: 192.168.192.241 7](#_Toc65396809)

[Service Enumeration 7](#_Toc65396810)

[Privilege Escalation 7](#_Toc65396811)

[3.3 House Cleaning 8](#_Toc65396812)

[Appendix – Any code snippets that were executed 9](#_Toc65396813)

# 1.0 Security Assessment Report

## 1.1 Introduction

The content of this course and the given tasks are for educational use only with aim to strengthen knowledge of students for practical approach in information gathering techniques.

Enjoy the time spent in lab and experiment as much as you can while respecting your fellow colleagues as this is shared environment.

## 1.2 Objective

The objective of students is to learn basic of active information gathering by working their way through a virtual lab of vulnerable by design virtual machines.

## 1.3 Requirements

The student should work individually on the given assessment taking into consideration the following requirements:

* Perform any active information gathering on the given target hosts only
* Do not run any automated tools with a broad band of network addresses which may cause network performance issues
* Each finding should be documented including screenshots, any code which was executed or payload which was used. (there should be at least one screenshot per box where you show two terminal windows – your attacker box with your IP address and the target box with IP address and user account level identifier)
* Any additional items if applicable
* Any uploaded exploits or tools must be removed, any traces which may leave your fingerprints should be cleaned (steps for these actions should be documented).

# 

# 2.0 High-Level Summary

Please summarize your work, approach and findings.

## 2.1 Recommendations

To be filled.

# 3.0 Methodologies

To be filled.

## 3.1 Information Gathering

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

**Lab Network**

* 192.168.192.231
* 192.168.192.241

## 3.2 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 ***2*** systems.

### System IP: 192.168.192.231

#### 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.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.192.231 | TCP: |
| UDP: |

**Nmap Scan Results:**

**Initial Shell Vulnerability Exploited**

***Additional info about where the initial shell was acquired from***

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Proof of Concept Code Here:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

### 

### System IP: 192.168.192.241

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.192.241 | TCP: |
| UDP: |

**Nmap Scan Results:**

**Initial Shell Vulnerability Exploited**

***Additional info about where the initial shell was acquired from***

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Proof of Concept Code Here:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

## 3.3 House Cleaning

To be documented.

# 

##### 

##### Appendix – Any code snippets that were executed

|  |
| --- |
|  |