OSCP Penetration Test Report

v.2.0

student@youremailaddress.com

OSID: XXXXX

A blue and purple circle with lines in it

Description automatically generated

Copyright © 2023 OffSec 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 OffSec.

[1. OffSec OSCP Exam Penetration Test Report 4](#_Toc161176883)

[1.1 Introduction 4](#_Toc161176884)

[1.2 Objective 4](#_Toc161176885)

[1.3 Requirements 4](#_Toc161176886)

[2. High-Level Summary 4](#_Toc161176887)

[2.1 Recommendations 5](#_Toc161176888)

[3. Methodologies 5](#_Toc161176889)

[3.1 Information Gathering 5](#_Toc161176890)

[3.2 Service Enumeration 6](#_Toc161176891)

[3.3 Penetration 6](#_Toc161176892)

[3.4 Maintaining Access 6](#_Toc161176893)

[3.5 House Cleaning 6](#_Toc161176894)

[4. Independent Challenges 8](#_Toc161176895)

[4.1 (Hostname) – (IP) 8](#_Toc161176896)

[4.1.3 Initial Access Summary – (Title of Exploit) 8](#_Toc161176897)

[4.1.2 Service Enumeration 8](#_Toc161176898)

[4.1.3 Initial Access – (Title) 8](#_Toc161176899)

[4.1.4 Post Exploitation – Local.txt 10](#_Toc161176900)

[4.1.5 Privilege Escalation Summary – (Title) 10](#_Toc161176901)

[4.1.6 Privilege Escalation – (Title) 10](#_Toc161176902)

[4.1.7 Post Exploitation – Proof.txt 11](#_Toc161176903)

[4.2 (Hostname) – (IP) 12](#_Toc161176904)

[4.2.1 Initial Access Summary – (Title of Exploit) 12](#_Toc161176905)

[4.2.2 Service Enumeration 12](#_Toc161176906)

[4.2.3 Initial Access – (Title) 12](#_Toc161176907)

[4.2.4 Post Exploitation – Local.txt 14](#_Toc161176908)

[4.2.5 Privilege Escalation Summary – (Title) 14](#_Toc161176909)

[4.2.6 Privilege Escalation – (Title) 14](#_Toc161176910)

[4.2.7 Post Exploitation – Proof.txt 15](#_Toc161176911)

[4.3 (Hostname) – (IP) 15](#_Toc161176912)

[4.3.1 Initial Access Summary – (Title of Exploit) 15](#_Toc161176913)

[4.3.2 Service Enumeration 16](#_Toc161176914)

[4.3.3 Initial Access – (Title) 16](#_Toc161176915)

[4.3.4 Post Exploitation – Local.txt 18](#_Toc161176916)

[4.3.5 Privilege Escalation Summary – (Title) 18](#_Toc161176917)

[4.3.6 Privilege Escalation – (Title) 18](#_Toc161176918)

[4.3.7 Post Exploitation – Proof.txt 19](#_Toc161176919)

[5. Active Directory Set 20](#_Toc161176920)

[5.1 (Hostname) – (IP) 20](#_Toc161176921)

[5.1.4 Post Exploitation – Local.txt 22](#_Toc161176922)

[5.1.5 Privilege Escalation Summary – (Title) 22](#_Toc161176923)

[5.1.6 Privilege Escalation – (Title) 23](#_Toc161176924)

[5.1.7 Post Exploitation – Proof.txt 24](#_Toc161176925)

[5.1.8 Post Exploitation – Lateral Movement 24](#_Toc161176926)

[5.2 (Hostname) – (IP) 25](#_Toc161176927)

[5.2.1 Initial Access Summary – (Title of Exploit) 25](#_Toc161176928)

[5.2.2 Service Enumeration 25](#_Toc161176929)

[5.2.3 Initial Access – (Title) 26](#_Toc161176930)

[5.2.4 Post Exploitation – Local.txt 27](#_Toc161176931)

[5.2.5 Privilege Escalation Summary – (Title) 27](#_Toc161176932)

[5.2.6 Privilege Escalation – (Title) 28](#_Toc161176933)

[5.2.7 Post Exploitation – Proof.txt 29](#_Toc161176934)

[5.2.8 Post Exploitation – Lateral Movement 29](#_Toc161176935)

[5.3 (Hostname) – (IP) 29](#_Toc161176936)

[5.3.1 Initial Access Summary – (Title of Exploit) 29](#_Toc161176937)

[5.3.2 Service Enumeration 29](#_Toc161176938)

[5.3.3 Post Exploitation – Proof.txt 29](#_Toc161176939)

[6. Proofs 31](#_Toc161176940)

[7. Appendix 32](#_Toc161176941)

# 1. OffSec OSCP Exam Penetration Test Report

## 1.1 Introduction

The OffSec Lab and Exam penetration test report contains all efforts that were conducted in order to pass the OffSec course. This report should contain all items that were used to pass the overall exam and it 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 OffSec Certified Professional.

## 1.2 Objective

The objective of this assessment is to perform an internal penetration test against the OffSec Lab and Exam network. The student is tasked with following a methodical approach to 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 in 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

John Doe was tasked with performing an internal penetration test towards OffSec Labs. 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 OffSec’s internal lab systems – the THINC.local domain. John’s overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to OffSec.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on OffSec’s network. When performing the attacks, John was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, John had administrative level access to multiple systems. All systems were successfully exploited and access granted.

ADD IN RELEVANT ISSUES TO THE SUMMARY e.g. weak password or exposed credentials

## 2.1 Recommendations

John recommends 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.

ADD IN RELEVANT FIXES TO THE RECCOMENDATIONS e.g. follow password policy or secure storage of credentials

# 3. Methodologies

John utilized a widely adopted approach to performing penetration testing that is effective in testing how well the OffSec Labs and Exam environments are secure. Below is a breakout of how John 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, John was tasked with exploiting the lab and exam network. The specific IP addresses were:

CHANGE IP ADDRESSES TO EXAM MACHINE IP’S

**Exam Network:**

192.168.232.55, 172.16.203.134, 172.16.203.135, 172.16.203.136

## 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, John was able to successfully gain access to x out of the 6 systems.

INDICATE HOW MANY MACHINES EXPLOITED

## 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.

John added administrator and root level accounts on all systems compromised. In addition to the administrative/root access, a msfvenom shell service was installed on the machine to ensure that additional access could be established.

## 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 organizations 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 the trophies on both the lab network and exam network were completed, John removed all user accounts and passwords added as well as the msfvenom shell services installed on the system. OffSec should not have to remove any user accounts or services from the system.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 4. Independent Challenges4.1 (Hostname) – (IP)4.1.3 Initial Access Summary – (Title of Exploit)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.1.2 Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.1.3 Initial Access – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.1.4 Post Exploitation – Local.txt **Machine IP and Local.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  4.1.5 Privilege Escalation Summary – (Title)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.1.6 Privilege Escalation – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.1.7 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  4.2 (Hostname) – (IP)4.2.1 Initial Access Summary – (Title of Exploit)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.2.2 Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.2.3 Initial Access – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.2.4 Post Exploitation – Local.txt **Machine IP and Local.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  4.2.5 Privilege Escalation Summary – (Title)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.2.6 Privilege Escalation – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.2.7 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  4.3 (Hostname) – (IP)4.3.1 Initial Access Summary – (Title of Exploit)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.3.2 Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.3.3 Initial Access – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.3.4 Post Exploitation – Local.txt **Machine IP and Local.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  4.3.5 Privilege Escalation Summary – (Title)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  4.3.6 Privilege Escalation – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  4.3.7 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  | |  | | 5. Active Directory Set **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP:**  **UDP:** | |  | **TCP:**  **UDP:** | |  | **TCP:**  **UDP:** |  5.1 (Hostname) – (IP) **5.1.1 Initial Access Summary – (Title of Exploit)**   |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |   **5.1.2 Service Enumeration**  **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |   **5.1.3 Initial Access – (Title)**   |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.1.4 Post Exploitation – Local.txt **Machine IP and Local.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  5.1.5 Privilege Escalation Summary – (Title)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  5.1.6 Privilege Escalation – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.1.7 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  5.1.8 Post Exploitation – Lateral Movement  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.2 (Hostname) – (IP)5.2.1 Initial Access Summary – (Title of Exploit)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  5.2.2 Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.2.3 Initial Access – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.2.4 Post Exploitation – Local.txt **Machine IP and Local.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  5.2.5 Privilege Escalation Summary – (Title)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  5.2.6 Privilege Escalation – (Title)  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.2.7 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  |  5.2.8 Post Exploitation – Lateral Movement  |  |  | | --- | --- | | **Command Ran:** |  | | **Description:** |  | | **Screenshot of command** |  |  5.3 (Hostname) – (IP)5.3.1 Initial Access Summary – (Title of Exploit)  |  |  | | --- | --- | | **Vulnerability Explanation:** |  | | **Vulnerability Fix:** |  | | **Severity:** |  | | **Steps to reproduce the attack:** |  | | **Link to Tools and Exploits Used:** |  |  5.3.2 Service Enumeration **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | |  | **TCP**:  **UDP**: |    5.3.3 Post Exploitation – Proof.txt **Machine IP and Proof.txt value:**   |  |  | | --- | --- | | **Command Ran:** |  | | **Screenshot of command** |  | | | |  |

# 6. Proofs

|  |  |  |
| --- | --- | --- |
| Machine IP | Local.txt | Proof.txt |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 7. Appendix

Modified Exploit Code: