Cisco And Evasion

Challenge by Théo ‘feloeht’ LEFEVRE

Étape 1: Téléchargement et Analyse de l’image.
L’énoncé nous parle d’un technicien ayant réalisé l’image d’un équipement suspect.
On peut soit s’attendre à une image disque, soit une image mémoire.

Après téléchargement de cette dernière, on se rend compte qu’il s’agit d'une archive compressée en gzip, on la dézippe.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ file device.img.gz
device.img.gz: gzip compressed data, was "device.img", last modified: Tue May 10 22:52:10 2022, max compression, from Un
ix, original size modulo 2^32 3166699520
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ gzip -dk device.img.gz
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ file device.img
device.img: Linux rev 1.0 ext4 filesystem data, UUID=99f9cf68-e6fa-4b90-aeee-7fa3e9ed5c2d, volume name "rootfs" (extents
) (large files)
```

On monte le filesystem:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ mkdir cisco && sudo mount -o loop device.img cisco
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ ls -la cisco/
total 84
drwxr-xr-x 19 root    root     4096 May 11 00:23 .
drwxrwxrwx  1 feloeht feloeht  4096 May 11 15:44 ..
lrwxrwxrwx  1 root    root        7 Apr  4 13:45 bin -> usr/bin
drwxr-xr-x  2 root    root     4096 Apr  4 14:05 boot
drwxr-xr-x  4 root    root     4096 Apr  4 13:45 dev
drwxr-xr-x 87 root    root     4096 May  8 18:38 etc
drwxr-xr-x  3 root    root     4096 Apr  4 14:07 home
lrwxrwxrwx  1 root    root        7 Apr  4 13:45 lib -> usr/lib
drwx------  2 root    root    16384 Apr  4 14:05 lost+found
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 media
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 mnt
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 opt
drwxr-xr-x  2 root    root     4096 Mar 27 05:33 proc
drwx------  3 root    root     4096 May  8 18:09 root
drwxr-xr-x  5 root    root     4096 Apr  4 13:50 run
lrwxrwxrwx  1 root    root        8 Apr  4 13:45 sbin -> usr/sbin
drwxr-xr-x  2 root    root     4096 Apr  4 13:45 srv
drwxr-xr-x  2 root    root     4096 Mar 27 05:33 sys
drwxrwxrwx  2 nobody  nogroup  4096 May 11 00:23 tftpboot
drwxrwxrwt  9 root    root     4096 May 10 01:00 tmp
drwxr-xr-x 11 root    root     4096 Apr  4 13:45 usr
drwxr-xr-x 11 root    root     4096 Apr  4 14:06 var
```

On cherche basiquement à se faire une idée de ce qu’il a pu se passer sur ce système:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la home/
total 12
drwxr-xr-x  3 root    root    4096 Apr  4 14:07 .
drwxr-xr-x 19 root    root    4096 May 11 00:23 ..
drwxr-xr-x  3 feloeht feloeht 4096 May 10 12:55 h4x0r
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la home/h4x0r/
total 142188
drwxr-xr-x 3 feloeht feloeht      4096 May 10 12:55 .
drwxr-xr-x 3 root    root         4096 Apr  4 14:07 ..
-rw------- 1 feloeht feloeht       647 May 10 12:19 .bash_history
-rw-r--r-- 1 feloeht feloeht       220 Apr  4 13:48 .bash_logout
-rw-r--r-- 1 feloeht feloeht      3523 Apr  4 13:48 .bashrc
drwxr-xr-x 3 feloeht feloeht      4096 May  8 18:05 .local
-rw-r--r-- 1 feloeht feloeht       807 Apr  4 13:48 .profile
-rw-r--r-- 1 feloeht feloeht       215 May  8 17:49 .wget-hsts
-rw-r--r-- 1 feloeht feloeht   5636152 May 10 12:53 capture.pcapng
-rw-r--r-- 1 feloeht feloeht 139921525 May  8 17:49 rockyou.txt
```

On remarque un peu d'activité dans le répertoire home de h4x0r, on décide d'en savoir un peu plus:

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat home/h4x0r/.bash_history
sudo apt install hydra-gtk
wget https://raw.githubusercontent.com/praetorian-inc/Hob0Rules/master/wordlists/rockyou.txt.gz
gzip -d rockyou.txt.gz
sudo hydra -p rockyou.txt 10.0.10.1 cisco
sudo apt install telnet
telnet 10.0.10.1
sudo apt install xinetd tftpd tftp
sudo nano /etc/xinetd.d/tftp
sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot
sudo /etc/init.d/xinetd start
telnet 10.0.10.1
sudo cp /tftpboot/sw-office-paris-confg /tftpboot/sw-office-paris-new
sudo nano /tftpboot/sw-office-paris-new
telnet 10.0.10.1
sudo apt-get install vlan tcpdump
sudo tcpdump -B 16096 -i eth1 -w capture.pcapng &feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$
```

A ce stade, on peut soit directement se diriger vers la finalité, et explorer la capture pcapng, ou alors on peut choisir d'en savoir un peu plus, et explorer différents fichiers référencés.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat etc/xinetd.d/tftp
service tftp
{
protocol        = udp
port            = 69
socket_type     = dgram
wait            = yes
user            = nobody
server          = /usr/sbin/in.tftpd
server_args     = /tftpboot
disable         = no
}
```

Ce fichier n'est autre qu'une configuration tftp, qui pointe vers le répertoire /tftpboot.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ ls -la tftpboot/
total 28
drwxrwxrwx  2 nobody nogroup 4096 May 11 00:23 
drwxr-xr-x 19 root   root    4096 May 11 00:23 ..
-rw-r--r--  1 root   root    8195 May  9 00:37 sw-office-paris-confg
-rw-r--r--  1 root   root    8186 May 10 12:55 sw-office-paris-new
```

Dans ce répertoire on trouve deux fichiers, on choisit de les étudier par date.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat tftpboot/sw-office-paris-confg
Current configuration : 8173 bytes
!
! Last configuration change at 00:55:46 UTC Mon Mar 1 1993 by cisco
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW-Office-Paris
!
boot-start-marker
boot-end-marker
!
!
```

Il s'agit d'un fichier de configuration d'un switch Cisco, qui a visiblement pu être récupéré suite à un bruteforce de l'interface d'administration telnet réalisée avec hydra et rockyou dans l'historique. On peut donc en déduire que le deuxième fichier contient cette configuration modifiée, on cherche donc à comprendre ce qui a été modifié.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ diff tftpboot/sw-office-paris-confg tftpboot/sw-office-paris-new
1,4d0
< Current configuration : 8173 bytes
< !
< ! Last configuration change at 00:55:46 UTC Mon Mar 1 1993 by cisco
< !
359a356,357
> monitor session 1 source vlan 10 both
> monitor session 1 destination interface GigabitEthernet0/47
```

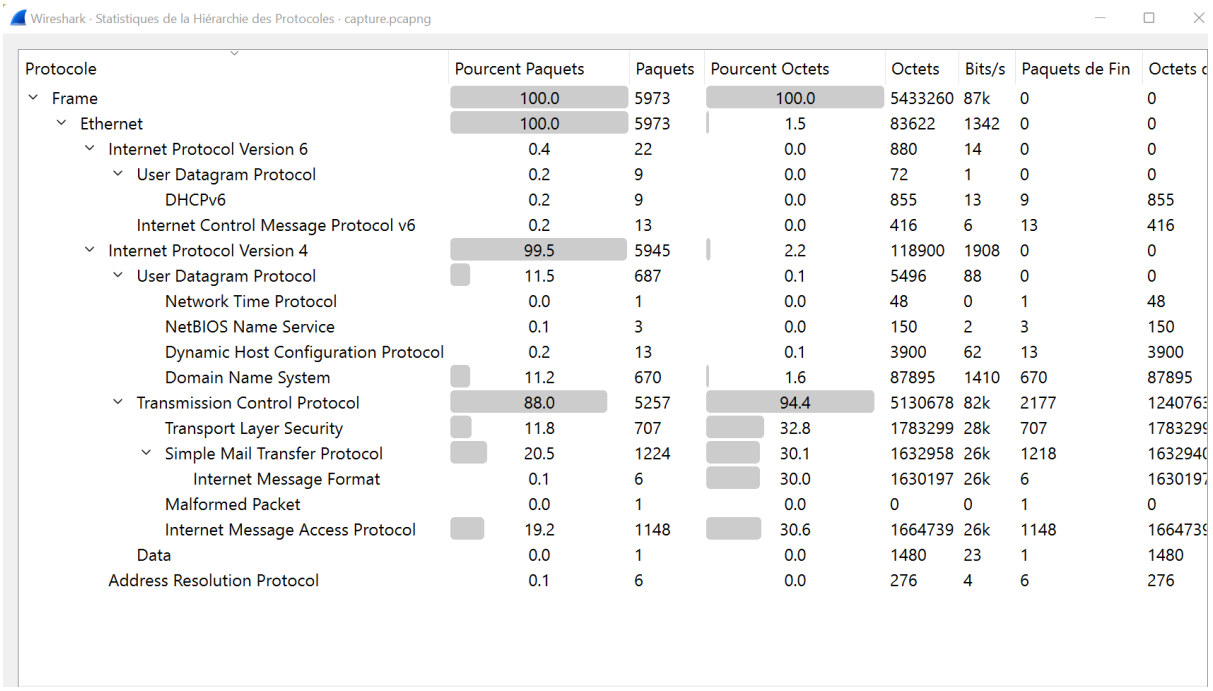
Hormis la suppression des commentaires de datage, on remarque l'ajout d'instructions de port-monitoring cisco, copiant tout le trafic du vlan 10 vers l'interface 47.
On peut donc en déduire qu'un équipement sniffer a été branché sur ce même port afin de récupérer le trafic du vlan 10.

```
interface Vlan10
 description SERVERS
 ip address 10.0.10.1 255.255.255.0
!
interface Vlan20
 description DIRECTION
 ip address 10.0.20.1 255.255.255.0
!
interface Vlan30
 description COLLABORATORS
 ip address 10.0.30.1 255.255.255.0
!
interface Vlan100
 description INTERCO-WAN
 ip address 172.16.100.100 255.255.255.0
!
ip default-gateway 172.16.100.254
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.100.254
!
```

D'après la précédente config, on découvre que le VLAN 10 est nommé VLAN SERVERS, il est donc question d'espionner le trafic à destination et au départ des serveurs (both).

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat home/h4x0r/.bash_history
sudo apt install hydra-gtk
wget https://raw.githubusercontent.com/praetorian-inc/Hob0Rules/master/wordlists/rockyou.txt.gz
gzip -d rockyou.txt.gz
sudo hydra -p rockyou.txt 10.0.10.1 cisco
sudo apt install telnet
telnet 10.0.10.1
sudo apt install xinetd tftpd tftp
sudo nano /etc/xinetd.d/tftp
sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot
sudo /etc/init.d/xinetd start
telnet 10.0.10.1
sudo cp /tftpboot/sw-office-paris-confg /tftpboot/sw-office-paris-new
sudo nano /tftpboot/sw-office-paris-new
telnet 10.0.10.1
sudo apt-get install vlan tcpdump
sudo tcpdump -B 16096 -i eth1 -w capture.pcapng &feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$
```

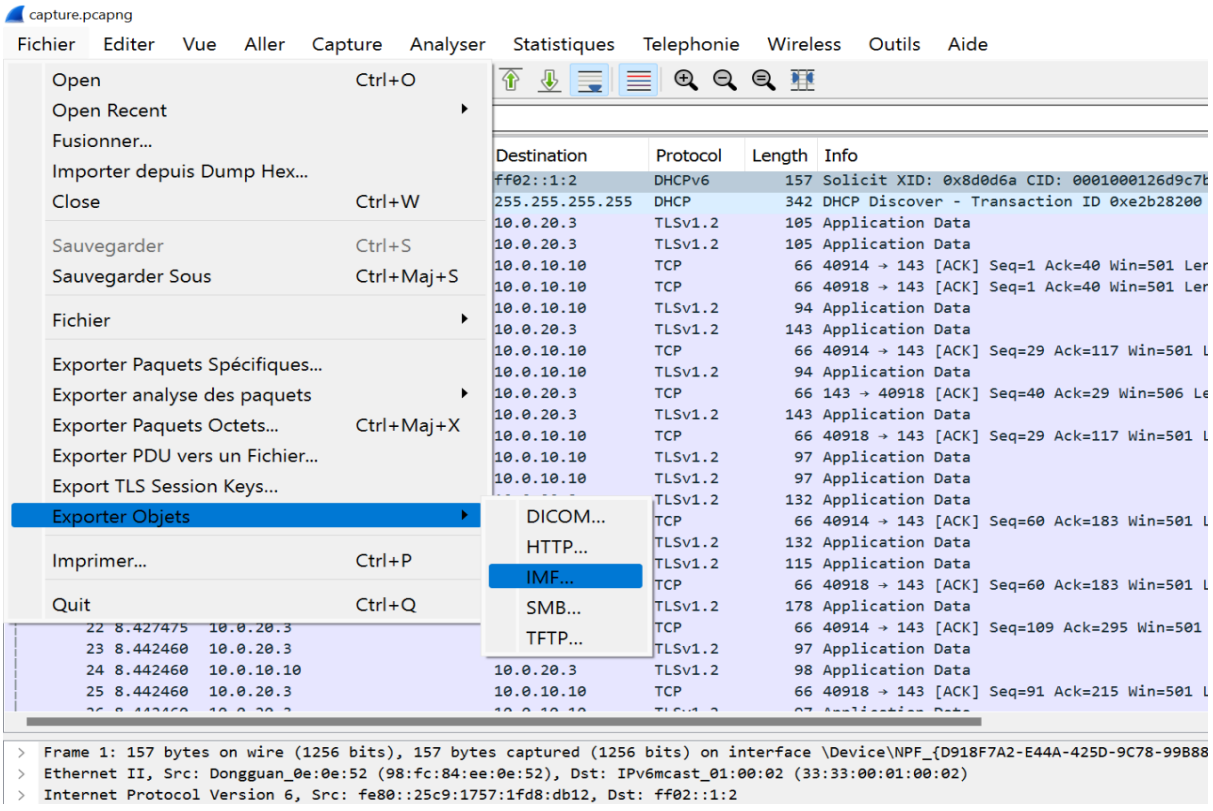
En se penchant à nouveau sur la config, on remarque l'exécution d'une capture réseau, enregistrée au sein du fichier capture.pcapng. Il semble donc judicieux de se pencher sur ce fichier.

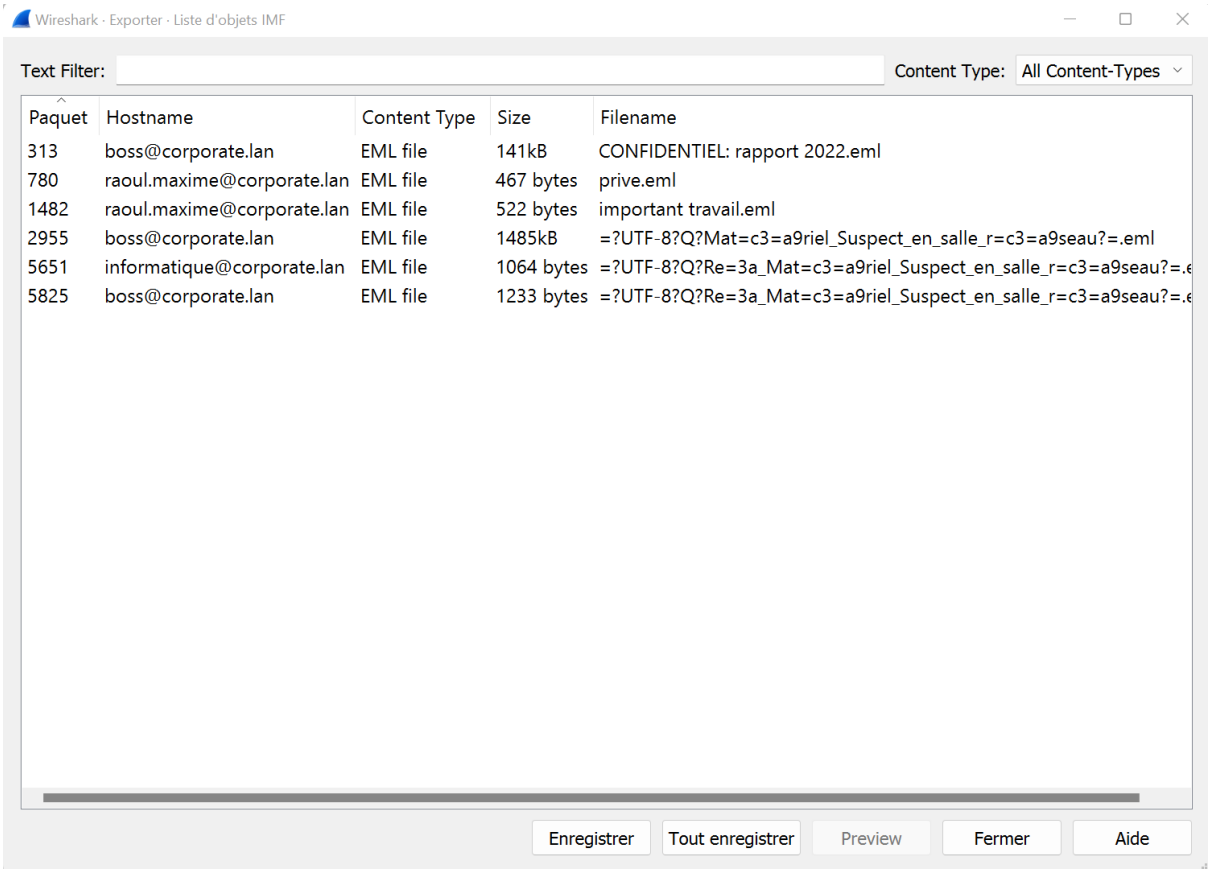


Protocole	Pourcent Paquets	Paquets	Pourcent Octets	Octets	Bits/s	Paquets de Fin	Octets d
Frame	100.0	5973	100.0	5433260	87k	0	0
Ethernet	100.0	5973	1.5	83622	1342	0	0
Internet Protocol Version 6	0.4	22	0.0	880	14	0	0
User Datagram Protocol	0.2	9	0.0	72	1	0	0
DHCPv6	0.2	9	0.0	855	13	9	855
Internet Control Message Protocol v6	0.2	13	0.0	416	6	13	416
Internet Protocol Version 4	99.5	5945	2.2	118900	1908	0	0
User Datagram Protocol	11.5	687	0.1	5496	88	0	0
Network Time Protocol	0.0	1	0.0	48	0	1	48
NetBIOS Name Service	0.1	3	0.0	150	2	3	150
Dynamic Host Configuration Protocol	0.2	13	0.1	3900	62	13	3900
Domain Name System	11.2	670	1.6	87895	1410	670	87895
Transmission Control Protocol	88.0	5257	94.4	5130678	82k	2177	124076
Transport Layer Security	11.8	707	32.8	1783299	28k	707	178329
Simple Mail Transfer Protocol	20.5	1224	30.1	1632958	26k	1218	163294
Internet Message Format	0.1	6	30.0	1630197	26k	6	163019
Malformed Packet	0.0	1	0.0	0	0	1	0
Internet Message Access Protocol	19.2	1148	30.6	1664739	26k	1148	166473
Data	0.0	1	0.0	1480	23	1	1480
Address Resolution Protocol	0.1	6	0.0	276	4	6	276

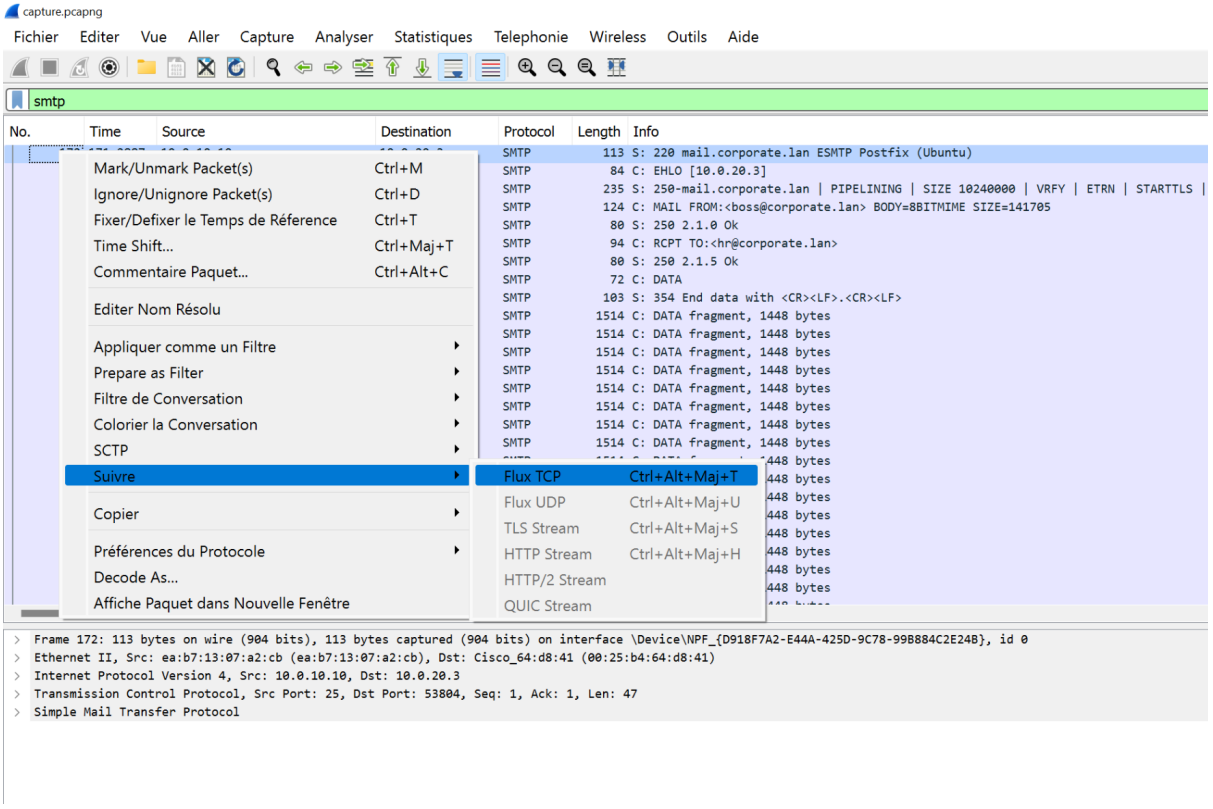
Une rapide analyse statistique des protocoles montre un usage important de TCP, UDP, DNS… mais rien de palpitant, cependant, on remarque la présence non négligeable de SMTP !

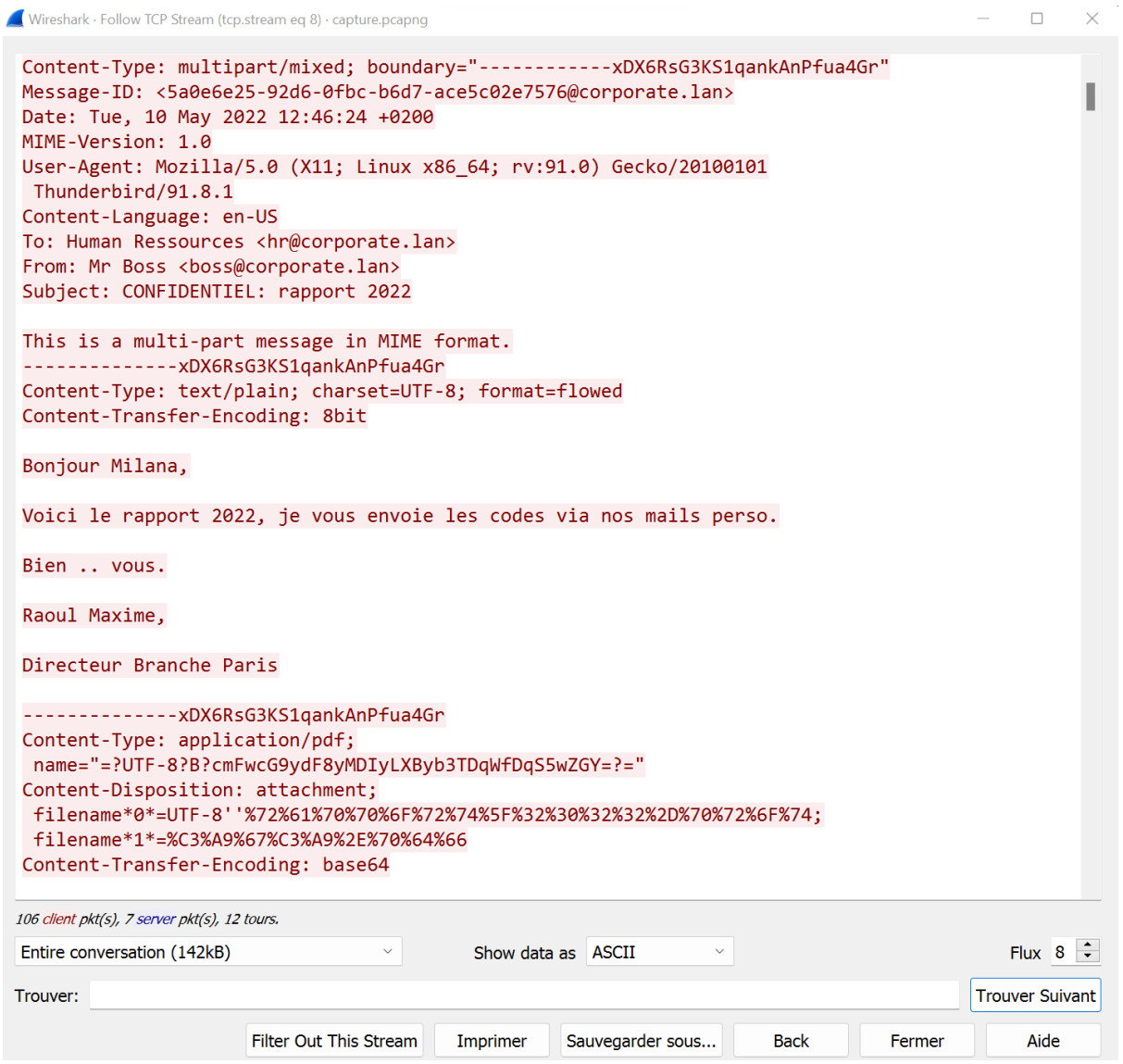
A ce stade là, deux solutions, soit on connaît les tricks et on passe par l'export d'objets, soit on retrace les trames SMTP afin d'en reconstituer automatiquement ou non les échanges.



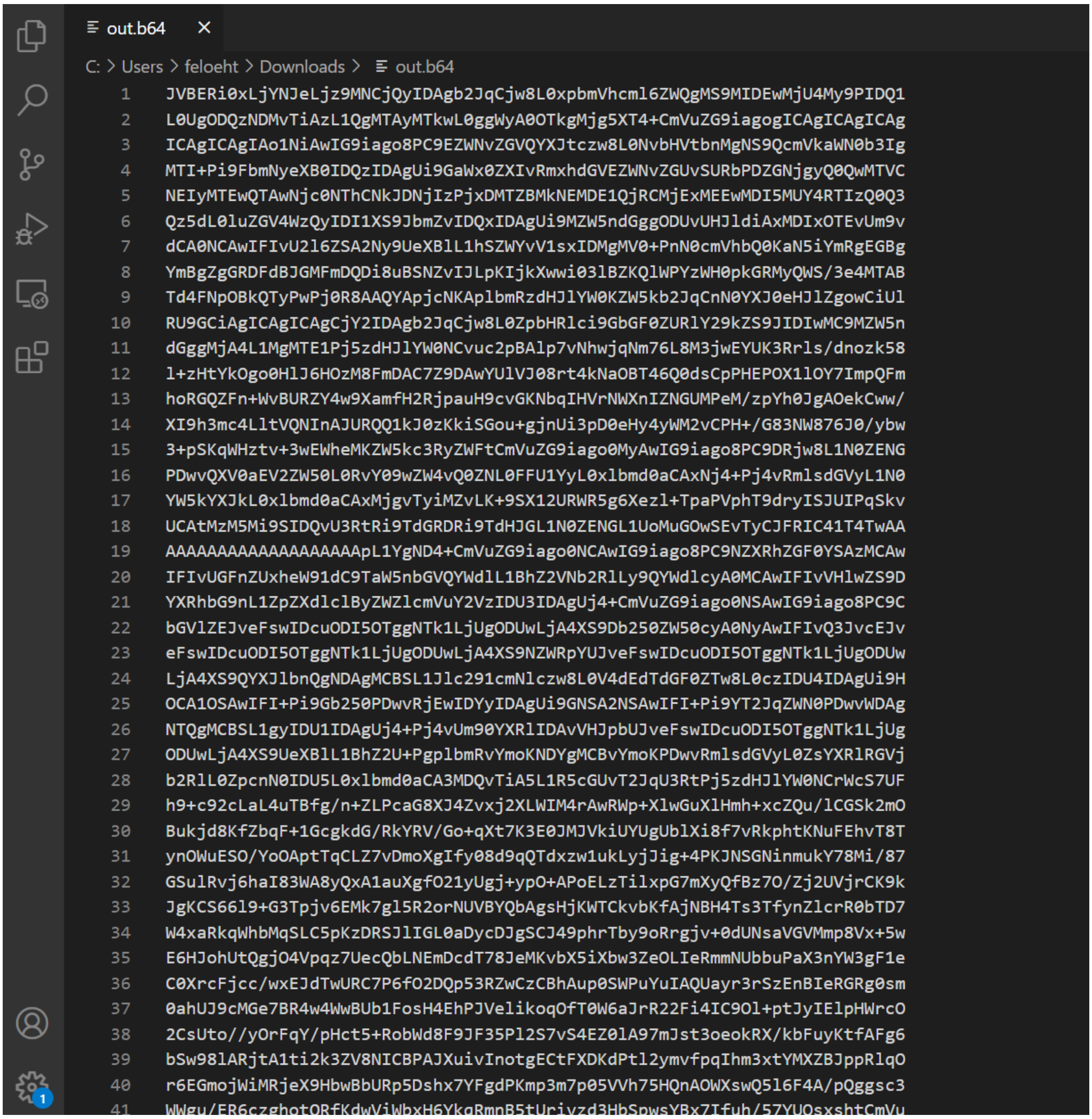


Avec cette solution on peut directement exporter les mails et continuer le challenge.
Voici la deuxième solution.

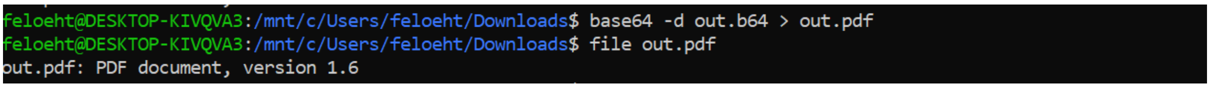




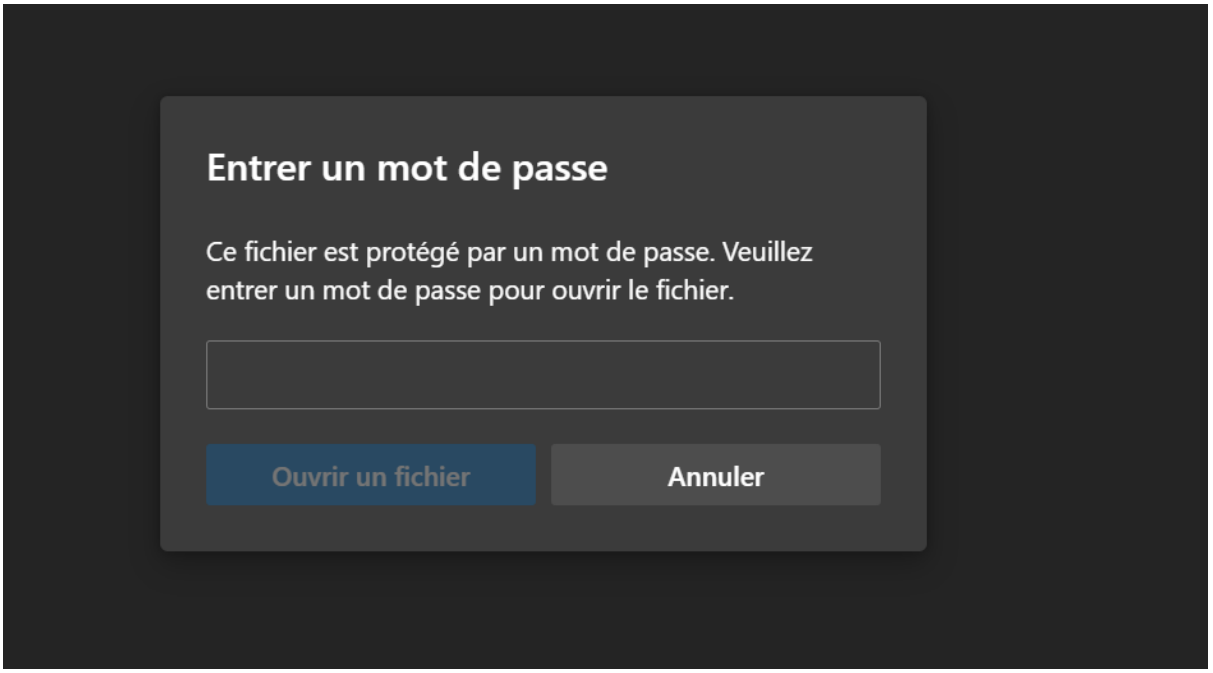
On peut désormais découvrir le contenu du premier message, qui semble contenir un fichier par mot de passe. Il est donc question d'extraire ce fichier, de la manière qui nous conviendra.
Une façon comme une autre de réaliser cela reste d'exporter la conversation en ASCII, ou en RAW, et de n'en garder que la partie contenant le fichier, encoder en base64.



Après suppression du reste du message, on conserve uniquement le code base64.



On obtient bien un PDF, ouvrons le !



Il est malheureusement protégé par mot de passe. On se souvient avoir lu que le mode de passe est envoyé dans un autre mail. Cherchons ce mail.

On trouve ainsi dans un autre échange le mot de passe en clair, qui nous permet d'ouvrir le PDF contenant le flag.

Le but de ce challenge est de montrer à la fois les problématiques liées à la sécurité physique d'un réseau, ainsi que l'importance d'utiliser des protocoles chiffrés, qui n'est à l'heure actuelle pas suffisamment le cas.