

Cisco And Evasion

Challenge by Théo 'feloeh't LEFEVRE

Step 1: Download and analyse the image.

The statement tells us about a technician who has taken an image of a suspect piece of equipment.

One can either expect a disk image or a memory image.

After downloading the latter, we realise that it is a gzip-compressed archive, we unzip it.

```
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/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 Unix, original size modulo 2^32 3166699520
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/Downloads$ gzip -dk device.img.gz
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/Downloads$ file device.img
device.img: Linux rev 1.0 ext4 filesystem data, UUID=99f9cf68-e6fa-4b90-aaaa-7fa3e9ed5c2d, volume name "rootfs" (extents) (large files)
```

We mount the filesystem:

```
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/Downloads$ mkdir cisco && sudo mount -o loop device.img cisco
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/Downloads$ ls -la cisco/
total 84
drwxr-xr-x 19 root root 4096 May 11 00:23 .
drwxrwxrwx 1 feloeh't feloeh't 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 tmp
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
```

We are basically trying to get an idea of what may have happened on this system:

```
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/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 feloeh't feloeh't 4096 May 10 12:55 h4x0r
feloeh't@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh't/Downloads/cisco$ ls -la home/h4x0r/
total 142188
drwxr-xr-x 3 feloeh't feloeh't 4096 May 10 12:55 .
drwxr-xr-x 3 root root 4096 Apr 4 14:07 ..
-rw----- 1 feloeh't feloeh't 647 May 10 12:19 .bash_history
-rw-r--r-- 1 feloeh't feloeh't 220 Apr 4 13:48 .bash_logout
-rw-r--r-- 1 feloeh't feloeh't 3523 Apr 4 13:48 .bashrc
drwxr-xr-x 3 feloeh't feloeh't 4096 May 8 18:05 .local
-rw-r--r-- 1 feloeh't feloeh't 807 Apr 4 13:48 .profile
-rw-r--r-- 1 feloeh't feloeh't 215 May 8 17:49 .wget-hsts
-rw-r--r-- 1 feloeh't feloeh't 5636152 May 10 12:53 capture.pcapng
-rw-r--r-- 1 feloeh't feloeh't 139921525 May 8 17:49 rockyou.txt
```

We notice some activity in the h4x0r home directory, so we decide to find out more:

```
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-config /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$
```

At this point, we can either go straight to the endpoint, and explore the pcapng capture, or we can choose to learn a little more, and explore different referenced files.

```
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
}
```

This file is just a tftp configuration, which points to the /tftpboot directory.

```
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-config
-rw-r--r--  1 root    root    8186 May 10 12:55 sw-office-paris-new
```

In this directory we find two files, we choose to study them by date.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads/cisco$ cat tftpboot/sw-office-paris-config
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
!
!
```

This is a configuration file for a Cisco switch, which could obviously be recovered following a bruteforce attack on the telnet administration interface using hydra and rockyou in the history. We can therefore deduce that the second file contains this modified configuration, so we are trying to understand what was modified.

```

feloeh@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh/Downloads/cisco$ diff tftpboot/sw-office-paris-config 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

```

Apart from the deletion of the dating comments, we note the addition of cisco port-monitoring instructions, copying all traffic from vlan 10 to interface 47.

We can therefore deduce that a sniffer device has been connected to this same port in order to retrieve the traffic from 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
!

```

According to the previous configuration, we discover that VLAN 10 is named VLAN SERVERS, it is thus a question of spying on the traffic to and from the servers (both).

```

feloeh@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh/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-config /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 &feloeh@DESKTOP-KIVQVA3:/mnt/c/Users/feloeh/Downloads/cisco$

```

If we look at the config again, we can see that a network capture is being executed, saved in the file capture.pcapng. It therefore seems sensible to look at this file.

Wireshark - Statistiques de la Hiérarchie des Protocoles - capture.pcapng

Protocole	Pourcent Paquets	Paquets	Pourcent Octets	Octets	Bits/s	Paquets de Fin	Octets c
▼ 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	1240763
Transport Layer Security	11.8	707	32.8	1783299	28k	707	1783299
▼ Simple Mail Transfer Protocol	20.5	1224	30.1	1632958	26k	1218	1632940
Internet Message Format	0.1	6	30.0	1630197	26k	6	1630197
Malformed Packet	0.0	1	0.0	0	0	1	0
Internet Message Access Protocol	19.2	1148	30.6	1664739	26k	1148	1664739
Data	0.0	1	0.0	1480	23	1	1480
Address Resolution Protocol	0.1	6	0.0	276	4	6	276

A quick statistical analysis of the protocols shows an important use of TCP, UDP, DNS... but nothing exciting, however, we notice the significant presence of SMTP!

At this stage, there are two solutions, either we know the tricks and we export objects, or we trace the SMTP frames in order to automatically reconstitute the exchanges or not.

capture.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Open Ctrl+O
Open Recent
Fusionner...
Importer depuis Dump Hex...
Close Ctrl+W
Sauvegarder Ctrl+S
Sauvegarder Sous Ctrl+Maj+S
Fichier
Exporter Paquets Spécifiques...
Exporter analyse des paquets
Exporter Paquets Octets... Ctrl+Maj+X
Exporter PDU vers un Fichier...
Export TLS Session Keys...
Exporter Objets
Imprimer... Ctrl+P
Quit Ctrl+Q

DICOM...
HTTP...
IMF...
SMB...
TFTP...

Destination	Protocol	Length	Info
ff02::1:2	DHCPv6	157	Solicit XID: 0x8d0d6a CID: 0001000126d9c7b
255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe2b28200
10.0.20.3	TLSv1.2	105	Application Data
10.0.20.3	TLSv1.2	105	Application Data
10.0.10.10	TCP	66	40914 → 143 [ACK] Seq=1 Ack=40 Win=501 Len=0
10.0.10.10	TCP	66	40918 → 143 [ACK] Seq=1 Ack=40 Win=501 Len=0
10.0.10.10	TLSv1.2	94	Application Data
10.0.20.3	TLSv1.2	143	Application Data
10.0.10.10	TCP	66	40914 → 143 [ACK] Seq=29 Ack=117 Win=501 Len=0
10.0.10.10	TLSv1.2	94	Application Data
10.0.20.3	TCP	66	143 → 40918 [ACK] Seq=40 Ack=29 Win=506 Len=0
10.0.20.3	TLSv1.2	143	Application Data
10.0.10.10	TCP	66	40918 → 143 [ACK] Seq=29 Ack=117 Win=501 Len=0
10.0.10.10	TLSv1.2	97	Application Data
10.0.10.10	TLSv1.2	97	Application Data
10.0.10.10	TLSv1.2	132	Application Data
10.0.10.10	TCP	66	40914 → 143 [ACK] Seq=60 Ack=183 Win=501 Len=0
10.0.10.10	TLSv1.2	132	Application Data
10.0.10.10	TLSv1.2	115	Application Data
10.0.10.10	TCP	66	40918 → 143 [ACK] Seq=60 Ack=183 Win=501 Len=0
10.0.10.10	TLSv1.2	178	Application Data
10.0.10.10	TCP	66	40914 → 143 [ACK] Seq=109 Ack=295 Win=501 Len=0
10.0.10.10	TLSv1.2	97	Application Data
10.0.10.10	TLSv1.2	98	Application Data
10.0.10.10	TCP	66	40918 → 143 [ACK] Seq=91 Ack=215 Win=501 Len=0
10.0.10.10	TLSv1.2	97	Application Data

> Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{D918F7A2-E44A-425D-9C78-99B88...}

> Ethernet II, Src: Dongguan_0e:0e:52 (98:fc:84:ee:0e:52), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)

> Internet Protocol Version 6, Src: fe80::25c9:1757:1fd8:db12, Dst: ff02::1:2

Wireshark · Follow TCP Stream (tcp.stream eq 8) · capture.pcapng

Content-Type: multipart/mixed; boundary="-----xDX6RsG3KS1qankAnPfua4Gr"
Message-ID: <5a0e6e25-92d6-0fbc-b6d7-ace5c02e7576@corporate.lan>
Date: Tue, 10 May 2022 12:46:24 +0200
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Thunderbird/91.8.1
Content-Language: en-US
To: Human Ressources <hr@corporate.lan>
From: Mr Boss <boss@corporate.lan>
Subject: CONFIDENTIEL: rapport 2022

This is a multi-part message in MIME format.
-----xDX6RsG3KS1qankAnPfua4Gr
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

Bonjour Milana,

Voici le rapport 2022, je vous envoie les codes via nos mails perso.

Bien .. vous.

Raoul Maxime,

Directeur Branche Paris

-----xDX6RsG3KS1qankAnPfua4Gr
Content-Type: application/pdf;
name="?UTF-8?B?cmFwcG9ydF8yMDIyLXByb3TDqWfDqS5wZGY=?"
Content-Disposition: attachment;
filename*0*=UTF-8''%72%61%70%70%6F%72%74%5F%32%30%32%32%2D%70%72%6F%74;
filename*1*=%C3%A9%67%C3%A9%2E%70%64%66
Content-Transfer-Encoding: base64

106 client pkt(s), 7 server pkt(s), 12 tours.

Entire conversation (142kB) Show data as ASCII Flux 8

Trouver: Trouver Suivant

Filter Out This Stream Imprimer Sauvegarder sous... Back Fermer Aide

We can now discover the contents of the first message, which seems to contain a password file. It is therefore a question of extracting this file, in a way that suits us.

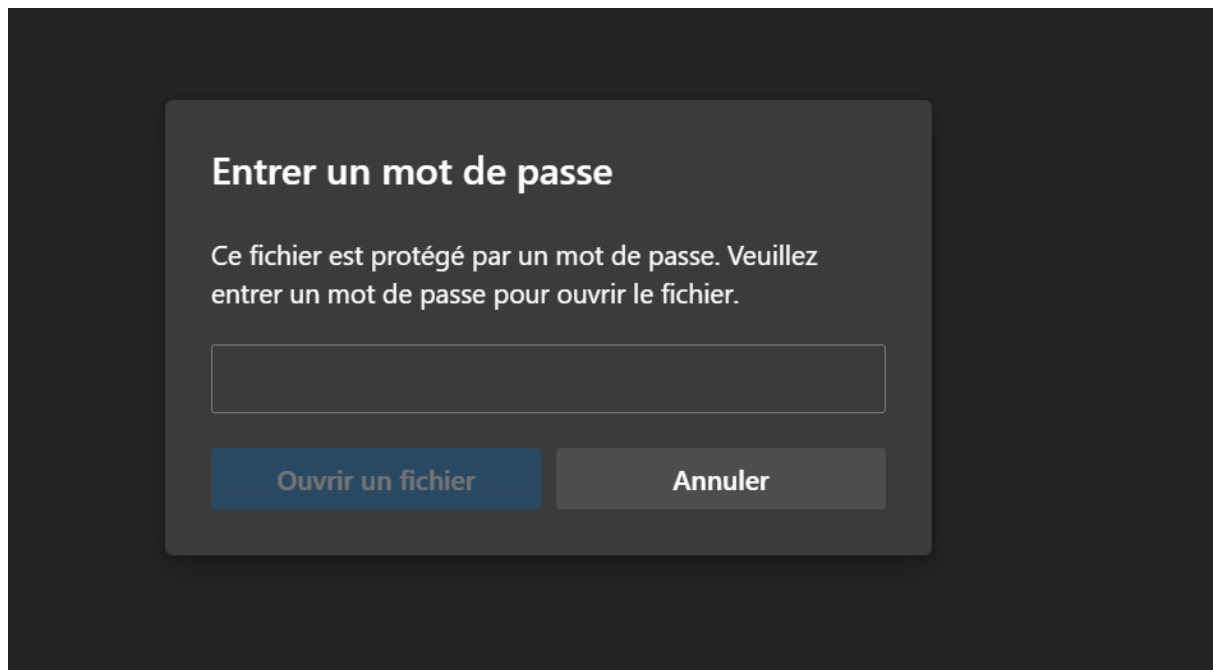
One way to do this is to export the conversation in ASCII, or RAW, and keep only the part containing the file, encoded in base64.


```
out.b64 X
C: > Users > feloeht > Downloads > out.b64
1 JVBBERi0xLjYnJelJz9MNCjQyIDAgb2JqCjw8L0xpbmVhcm16ZWQgMS9MIDEwMjU4My9PIDQ1
2 L0UgODQzNDMvTiAzL1QgMTAyMTkwL0ggWwA0OTkgMjg5XT4+CmVuZG9iagogICAgICAgICAg
3 ICAGICAgIAo1NiAwIG9iag08PC9EZWNvZGVQYXJtczw8L0NvbHVtbnMgNS9QcmVkaWN0b3I
4 MTI+Pi9FbmNyeXB0IDQzIDAgUi9GaWx0ZXIvRmxdGVEZWNvZGUvSURbPDZGNjgyQ0QwMTVC
5 NEIyMTEwQTAWNjc0NThCNkJDNDJzPjxDMTZBMkNEMDE1QjRCMjExMEEwMDI5MUUY4RTIzQ0Q3
6 Qz5dL0l1uZGV4WzQyIDI1XS9JbmZvIDQxIDAgUi9MZW5ndGggODUvUHJldiAxMDIxOTEvUm9v
7 dCA0NCAwIFiVU2l6ZSA2Ny9UeXB1L1hsZWYvV1sxIDMgMV0+PnN0cmVhbQ0KaNSiYmRgEGBg
8 YmBgZgGRDFdBjGMFMDQDi8uBSNZvIjLpKIjKXwwi03lBZKQlWPYzWH0pkGRMyQWS/3e4MTAB
9 Td4FNpOBKQTyPwPj0R8AAQYApjcNKAplbmRzdHJlYW0KZW5kb2JqCnN0YXJ0eHJlZgowCiU1
10 RU9GCGiAgICAgICAgCjY2IDAgb2JqCjw8L0ZpbHRlc9iG6GfGF0ZURlY29kZS9JIDIwMCMZW5n
11 dGggMjA4L1MgMTE1Pj5zdHJlYW0NCvuc2pBa1p7vNhwjqNm76L8M3jwEYUK3Rr1s/dnozK58
12 1+zHtYkOgo0HlJ6HOzM8FmDAC7Z9DAwYU1VJ08rt4kNaOBT46Q0dsCpPHEPOX110Y7ImpQMf
13 hoRGQZFh+WvBURZY4w9XamfH2RjpauH9cvGKNbqIHvRNWxNIZNGUMPem/zpYh0JgAOekCww/
14 XI9h3mc4L1tVQNIaJURQQ1kJ0zKkiSGou+gjnUi3pD0eHy4yWM2vCPH+/G83NW876J0/ybw
15 3+pSKqWHztv+3wEwheMKZW5kc3RyZWFTcmVuZG9iag0MyAwIG9iag08PC9DRjw8L1N0ZENG
16 PDwvQXV0aEV2ZW50L0RvY09wZW4vQ0ZNL0FFU1YyL0xlbmd0aCAxNj4+Pj4vRmlsdGvYlL1N0
17 YW5kYXJkL0xlbmd0aCAxMjg5YmZvIDU3IDAgUj4+CmVuZG9iag0NSAwIG9iag08PC9C
18 UCAtMzMS5iS9IDQvU3RtRi9TdGRDRi9TdHJGL1N0ZENGL1UoMuG0wSEvTyCjFRIC41T4TwAA
19 AAAAAAAAAAAAAAAAAAPlYgND4+CmVuZG9iag0NCAwIG9iag08PC9NZXRhZGF0YSAzMCAw
20 IFiVUGFnZUxheW91dC9Taw5nbGVQYwdlL1BhZ2Vnb2RlYy9QYwdlcyA0MCAwIFiVHlWZS9D
21 YXRhbG9nL1ZpZXdlc1ByZWZlcmVuY2VzIDU3IDAgUj4+CmVuZG9iag0NSAwIG9iag08PC9C
22 bGV1ZEJveFswIDcuODI5OTggNTk1LjUgODUwLjA4XS9Db250ZW50cyA0NyAwIFiVQ3JvcEJv
23 eFswIDcuODI5OTggNTk1LjUgODUwLjA4XS9NZWRpYUJveFswIDcuODI5OTggNTk1LjUgODUw
24 LjA4XS9QYXJlbnQgNDAgMCSL1Jlc291cmNlc2w8L0V4dEdTdGF0ZTw8L0czIDU4IDAgUi9H
25 OCA1OSAwIFi+Pi9G6b250PDwvRjEwIDYyIDAgUi9GNSA2NSAwIFi+Pi9YT2JqZWNoPDwvWD
26 NTQgMCSL1gyIDU1IDAgUj4+Pj4vUm90YXRlIDAvVHJpbUJveFswIDcuODI5OTggNTk1LjUg
27 ODUwLjA4XS9UeXB1L1BhZ2U+PgplbmRvYmoKNDYgMCSvYmoKPDwvRmlsdGvYl0ZsYXRlRGVj
28 b2RlL0ZpcnN0IDU5L0xlbmd0aCA3MDQvTiA5L1R5cGUvT2JqU3RtPj5zdHJlYW0NCrWcS7UF
29 h9+c92clala4uTBfg/n+ZLPcaG8XJ4Zvxj2XLWIM4rAwRWp+XlwGuXlHmh+xcZQu/1CGSk2mO
30 Bukjd8KfZbqF+1GcgkdG/RkYRV/Go+qXt7K3E0JMjVkiUYUgUblXi8f7vRkphTknUEhvT8T
31 yn0WuESO/YoAptTqCLZ7vDmoXgIfy08d9qQTdxzw1ukLyjJig+4PKJNSGNinmukY78Mi/87
32 GSulRvj6haI83WA8yQxA1auXgf021yUgj+yp0+APoELzTilxpG7mXyQfBz70/Zj2UVjrCK9k
33 JgKCS66l9+G3Tpjv6EMk7g15R2orNUVBQbAgsHjKWTCkvbKfAjNBH4Ts3TfynZlcrR0bTD7
34 W4xaRkqWhbMqSLC5pKzDRSJ1IGL0aDycDJGSCJ49phrTby9oRrgjv+0dUNsaVGVVmp8Vx+5w
35 E6HJohUtQgj04Vpqz7UecQbLNEmDcdT78JeMKvbX5iXbw3ZeOLIErmmNUbbuPaX3nYW3Gf1e
36 C0XrcFjcc/wxEjdTwURC7P6f02DQp53RZwCzCBhAup0SWPuYIAQUayr3rSzEnBIErGRg0sm
37 0ahUJ9cMGe7BR4w4WwBub1FosH4EhPJVeIikoqOfT0W6aJrR22Fi4IC90l+ptJyIElPHWrcO
38 2CsUto//yOrFqY/pHct5+RobWd8F9JF35P12S7vS4EZ0lA97mJst3oeokRX/kbFuyKtFAFg6
39 bSw98lARjtA1ti2k3ZV8NICBPAJXuivInotgECtFXDKdPt12ymvfpqIhm3xtYMXZBJppRlQ0
40 r6EGmojWiMRjeX9HbwBbURp5Dshx7YFgdPKmp3m7p05VVh75HQnAOWXswQ5l6F4A/pQggsc3
41 Wwgu/ER6czphotQRfKdwViWbxH6YkqRmpB5tUnivzd3HbSpwsYBx7Tfuh/57YU0sxshtCmVu
```

After deleting the rest of the message, only the base64 code remains.

```
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ base64 -d out.b64 > out.pdf
feloeht@DESKTOP-KIVQVA3:/mnt/c/Users/feloeht/Downloads$ file out.pdf
out.pdf: PDF document, version 1.6
```

We get a PDF, let's open it!



Unfortunately it is password protected. We remember reading that the password is sent in another email. Let's look for this email.

We find in another exchange the password in clear text, which allows us to open the PDF containing the flag.

The aim of this challenge is to show both the problems linked to the physical security of a network, as well as the importance of using encrypted protocols, which is currently not sufficiently the case.