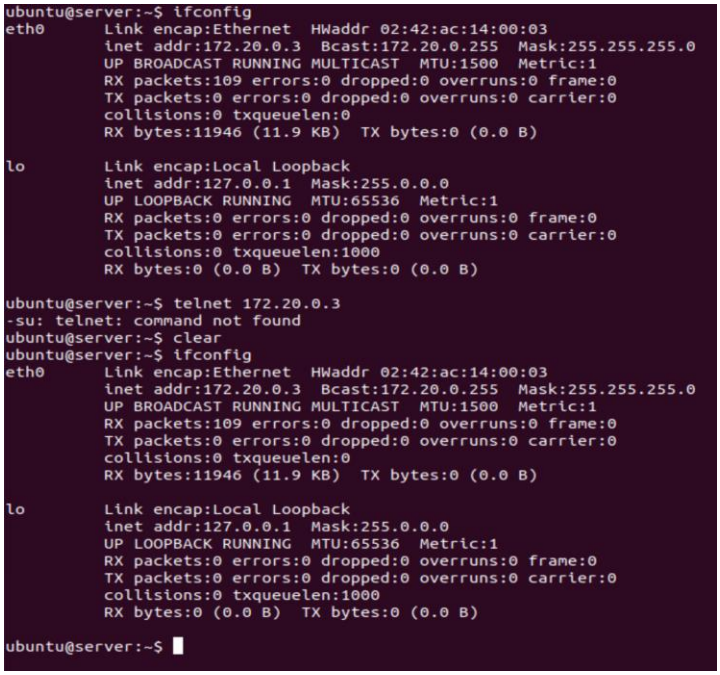
TD Cybersécurité n°1

Etape 1 : on tape la commande *ifconfig* pour avoir l'adresse IP du serveur.



Etape 2 : Sur le terminal du client on tape la commande telnet *< IP du serveur >* pour pouvoir accéder au fichier du serveur. Ensuite on se connecte aevc le username *ubuntu* et le mot de passe *ubuntu*.

Une fois dedans, on tape la commande *ls* pour afficher la liste des fichiers présents sur le serveur puis on tape la commande *cat < filetoview.txt >* .

```
ubuntu@client:~$ telnet 172.20.0.3
Trying 172.20.0.3...
Connected to 172.20.0.3.
Escape character is '^]'.
Ubuntu 16.04.4 LTS
server login: ubuntu
Password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ubuntu@server:~$ ls
filetoview.txt
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) cont
ainer

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: ea2b5d5065c6332eb563e0e3d96efa63
ubuntu@server:~$ exit
logout
Connection closed by foreign host.
ubuntu@client:~$
```

Etape 3 : Sur le serveur on tape la commande *sudo tcpdump –i eth0 –x tcp*

```
student@LabtainersVM:~$ sudo tcpdump -i eth0 -x tcp
```

Ensuite sur le client on démarre une session telnet *<IP du serveur>* et on fait exprès de rentrer un faux mot de passe. Puis on observe le flux *tcpdump* du serveur sur le terminal du serveur. On remarque que le mot de passe apparait en clair sur le serveur.

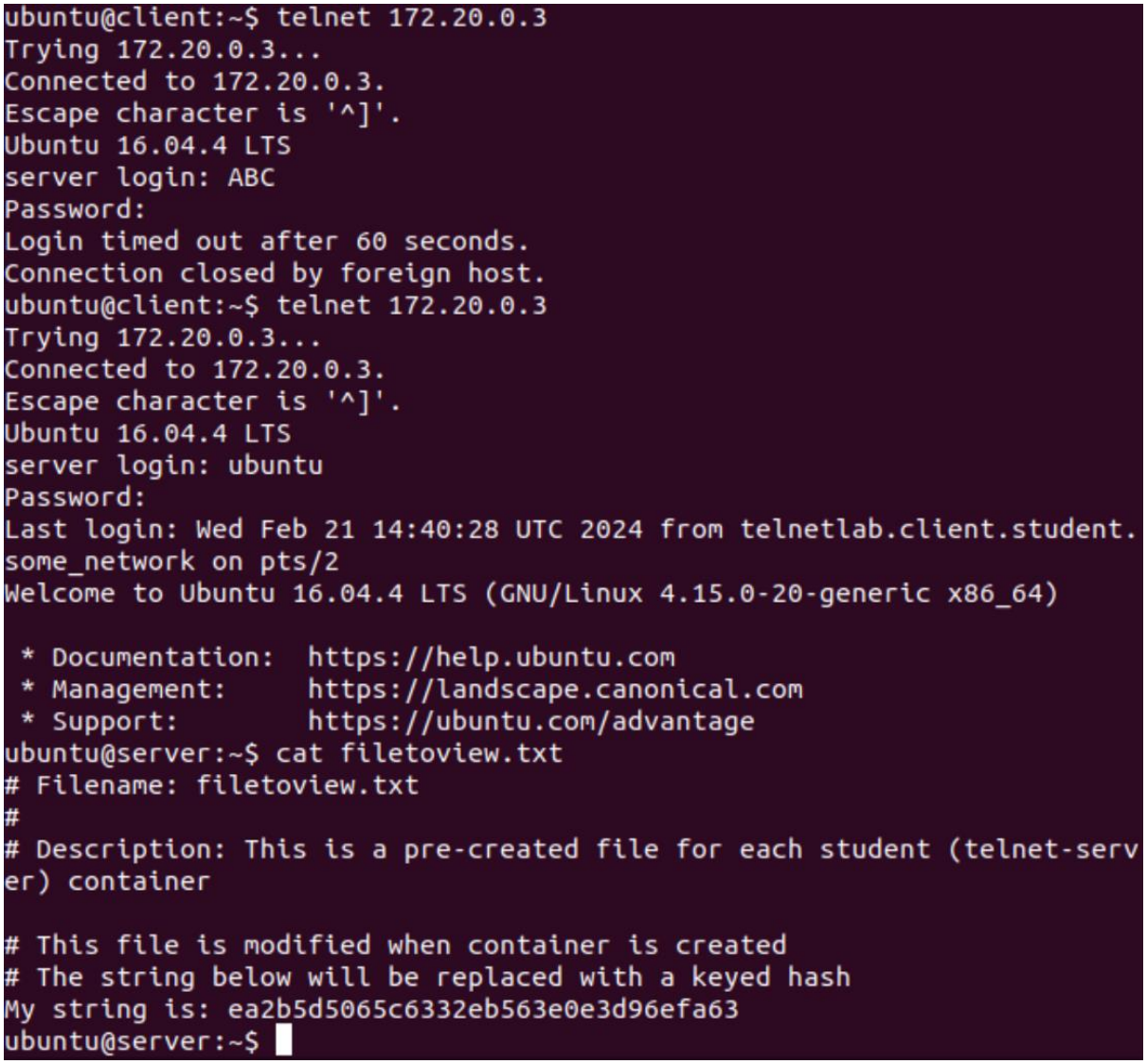
```
ubuntu@client:~$ telnet 172.20.0.3
Trying 172.20.0.3...
Connected to 172.20.0.3.
Escape character is '^]'.
Ubuntu 16.04.4 LTS
server login: ABC
Password:
Login timed out after 60 seconds.
Connection closed by foreign host.
ubuntu@client:~$
```

```
^Cubuntu@server:~$
39 packets captured
39 packets received by filter
0 packets dropped by kernel
n
3
```

```
14:53:21.923784 IP server.telnet > telnetlab.client.student.some_network.60760:
 Flags [P.], seq 92:93, ack 109, win 227, options [nop,nop,TS val 3512423815 ec
r 338217041], length 1
        0x0000:  4510 0035 8856 4000 4006 5a2f ac14 0003
        0x0010:  ac14 0002 0017 ed58 3e63 3397 3bbc a714
        0x0020:  8018 00e3 5855 0000 0101 080a d15b 5587
        0x0030:  1428 c851 41
14:53:21.923804 IP telnetlab.client.student.some_network.60760 > server.telnet:
 Flags [.], ack 93, win 229, options [nop,nop,TS val 338217042 ecr 3512423815],
 length 0
        0x0000:  4510 0034 1ddf 4000 4006 c4a7 ac14 0002
        0x0010:  ac14 0003 ed58 0017 3bbc a714 3e63 3398
        0x0020:  8010 00e5 5854 0000 0101 080a 1428 c852
        0x0030:  d15b 5587
```

Ensuite on recommence la même chose mais en mettant cette fois ci le bon mot de passe puis on effectue un *cat filetoview.txt.*

On observe que le contenue du fichier apparait en brut sur le serveur (*tcpdump).*



Etape 4 : Sur le client, on tape la commande *ssh < IP serveur >.*

La connexion ne s'effectue pas la première fois mais on peut vérifier que la clé SHA256 correspond bien à celle du serveur.

Ensuite on accepte l'invitation puis on affiche le contenu du fichier.

On observe la sortie *tcpdump* sur le serveur et je constate que le fichier n’est plus lisible en brut.