

TP n° 1 - M3102 - Installation et configuration de services courants

## **SOMMAIRE**

<b>I - Configuration du réseau.....</b>	<b>2</b>
<b>II - Installation et configuration de services.....</b>	<b>5</b>
<b>III - Analyse de trafic et sécurité des échanges.....</b>	<b>11</b>

## **LIEN VERS LE SUJET DE TP**

## I - Configuration du réseau

### 1) Création de la machine virtuelle

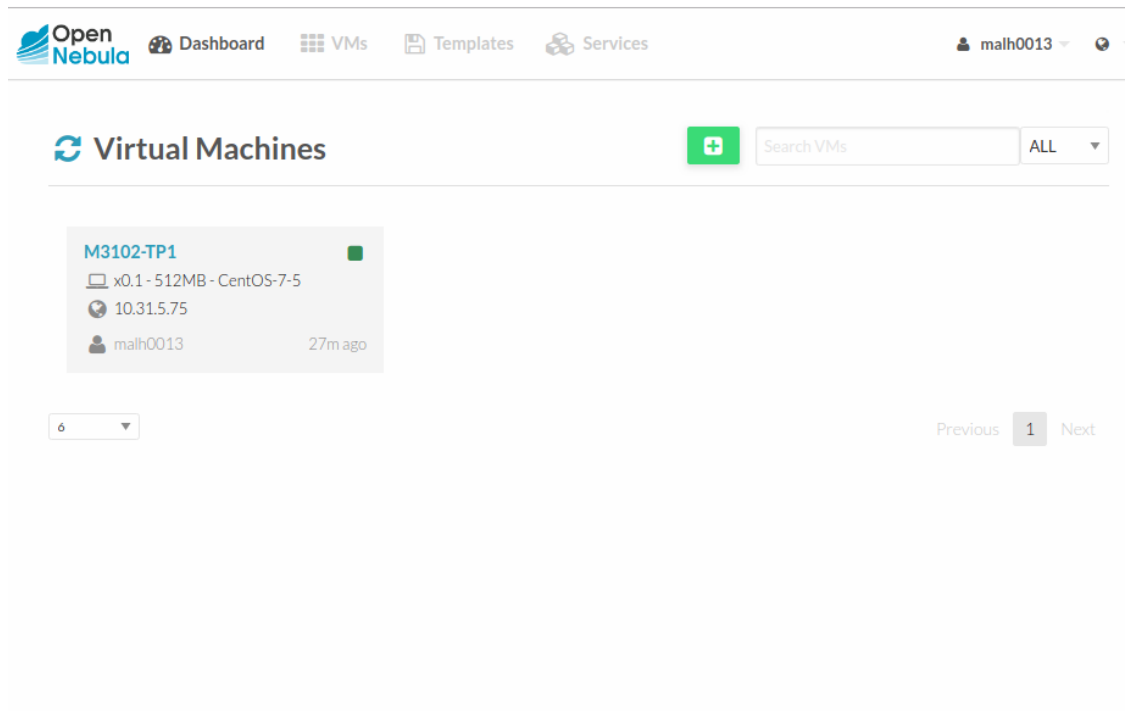


Illustration 1: Création de la machine virtuel sur OpenNebula

### 2) Connexion sur le serveur

```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.14.1.el7.x86_64 on an x86_64

localhost login: root
Password:
Last login: Thu Sep 19 11:00:30 from pc088.iut-rcc-info.urca
[root@localhost ~]#
```

Illustration 2: Connexion au serveur via le terminal sur Ubuntu

### 3) Connexion depuis un poste de travail

```
malh0013@2A4F1-31UPC088:/home/Etudiants/malh0013$ ssh -l root 10.31.5.75
root@10.31.5.75's password:
Last login: Thu Sep 19 10:48:09 2019 from pc088.iut-rcc-info.urca
[root@localhost ~]# useradd charles
[root@localhost ~]# passwd charles
Changement de mot de passe pour l'utilisateur charles.
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Les mots de passe ne correspondent pas.
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mise à jour réussie de tous les jetons d'authentification.
```

Illustration 3: Création d'un utilisateur

### 4) Rappel : base de comptes locale

```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:30:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
avahi-autoipd:x:170:
ssh_keys:x:999:
systemd-journal:x:190:
dbus:x:81:
polkitd:x:998:
tss:x:59:
dip:x:40:
postdrop:x:90:
postfix:x:89:
sshd:x:74:
user1:x:1000:
charles:x:1001:
```

Illustration 4: Affichage du fichier /etc/group

```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
user1:x:1000:1000:/:/home/user1:/bin/bash
charles:x:1001:1001:/:/home/charles:/bin/bash

```

Illustration 5: Affichage du fichier /etc/passwd

```

root:$6$CdYj0/Ha$FE.Z74wZfIjX69FgIGWbLDElQdzktDxJFo8KIQpgjp32Zw1Jm5h0iDHHV7U1.tHNo1X0xonk8I8Vzyy8jkzPt0:18158:0:99999:7:::
bin:!:16372:0:99999:7:::
daemon:!:16372:0:99999:7:::
adm:!:16372:0:99999:7:::
lp:!:16372:0:99999:7:::
sync:!:16372:0:99999:7:::
shutdown:!:16372:0:99999:7:::
halt:!:16372:0:99999:7:::
mail:!:16372:0:99999:7:::
operator:!:16372:0:99999:7:::
games:!:16372:0:99999:7:::
ftp:!:16372:0:99999:7:::
nobody:!:16372:0:99999:7:::
avahi-autoipd:!:16722:0:0:0:
dbus:!:16722:0:0:0:
polkitd:!:16722:0:0:0:
tss:!:16722:0:0:0:
postfix:!:16722:0:0:0:
sshd:!:16722:0:0:0:
user1:$6$00ItV70l$NivLh.S2jDTpfvsyzb9uz2XPv5nILSesvV1Z0mv630lap7UwA.02DT5SdeuqLTSHnqvbUPNC2w.jsRdXYV1Ay0:18158:0:99999:7:::
charles:$6$AJP0qkI6$plHyceykwjjPWEv6E0UICARLwiTetPaHhJjmEsd0mqjT/wBwBw2J.hdLZNokTYHKhmJIKo08i/biiod9Vs0h/:18158:0:99999:7:::

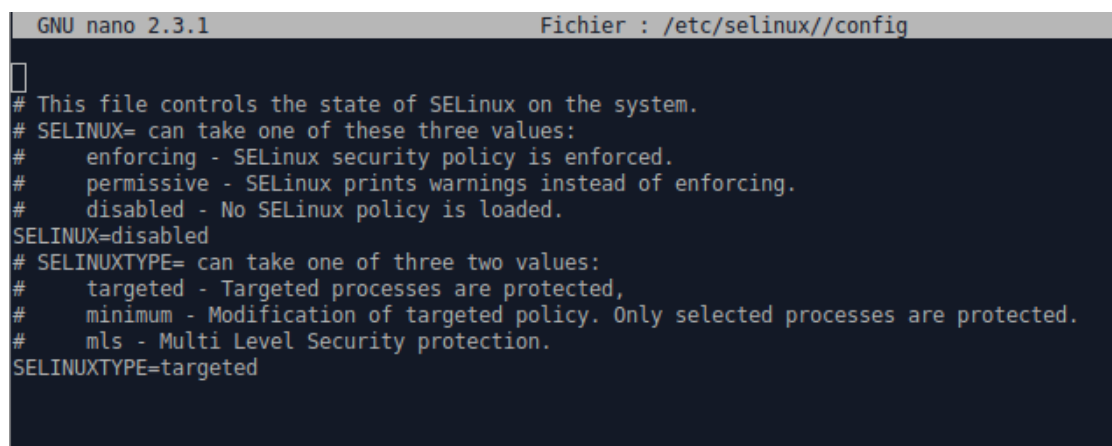
```

Illustration 6: Affichage du fichier /etc/group

## II - Installation et configuration de services

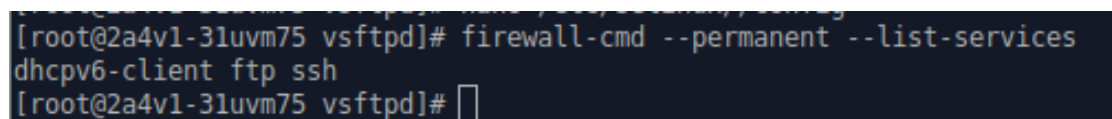
### 1) Le service ftp

#### a) Installation e vsftpd



```
GNU nano 2.3.1 Fichier : /etc/selinux//config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Illustration 7: Désactivation de SELINUX dans le fichier de configuration



```
[root@2a4v1-3lsvm75 vsftpd]# firewall-cmd --permanent --list-services
dhcpv6-client ftp ssh
[root@2a4v1-3lsvm75 vsftpd]#
```

Illustration 8: Ajout des ports du service ftp au firewall

Tester la connexion avec le client ftp de Linux ou de Windows (modeCLI) et FileZilla. Tenter de parcourir l'arborescence ...

La connexion avec le client ftp fonctionne et il est possible de parcourir l'arborescence (voir captures d'écrans ci-dessous).

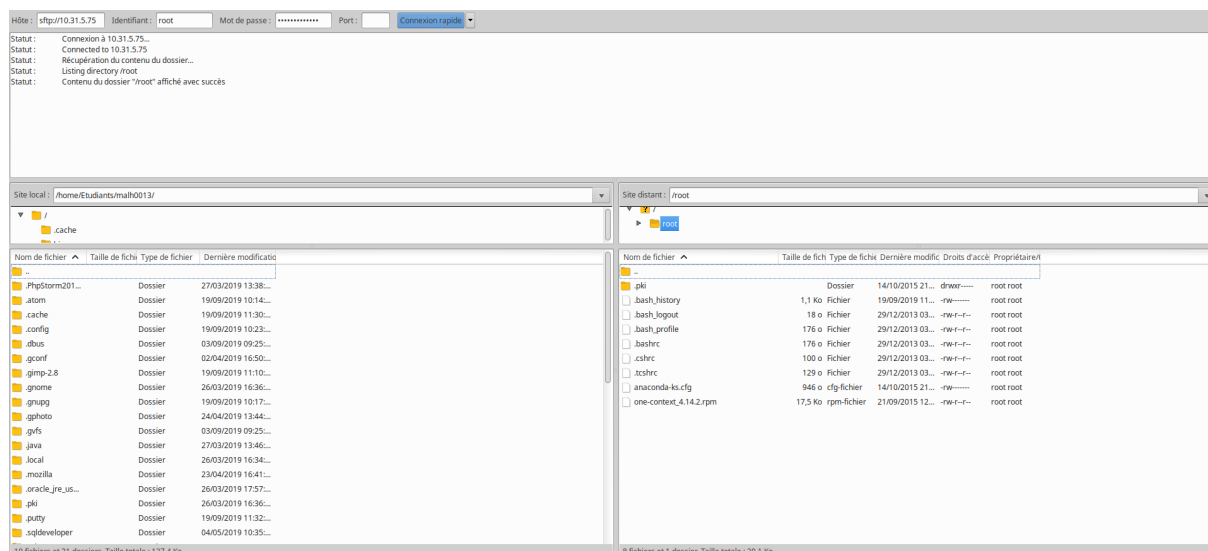


Illustration 9: Connexion via un client ftp avec les compte Root

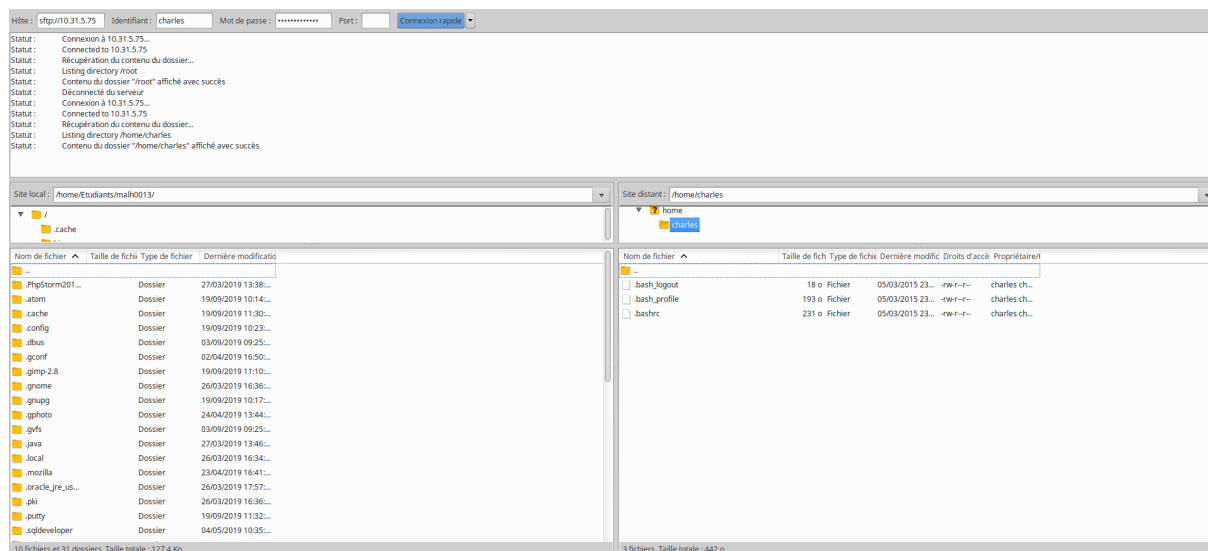


Illustration 10: Connexion via un client ftp avec le compte Charles

## b) Sécurisation du service

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
```

Illustration 11: Activation de la directive chroot

Tenter à nouveau de parcourir l'arborescence...

Cela affiche désormais un message d'erreur quand on souhaite parcourir l'arborescence avec la directive `chroot_local_user` activée.

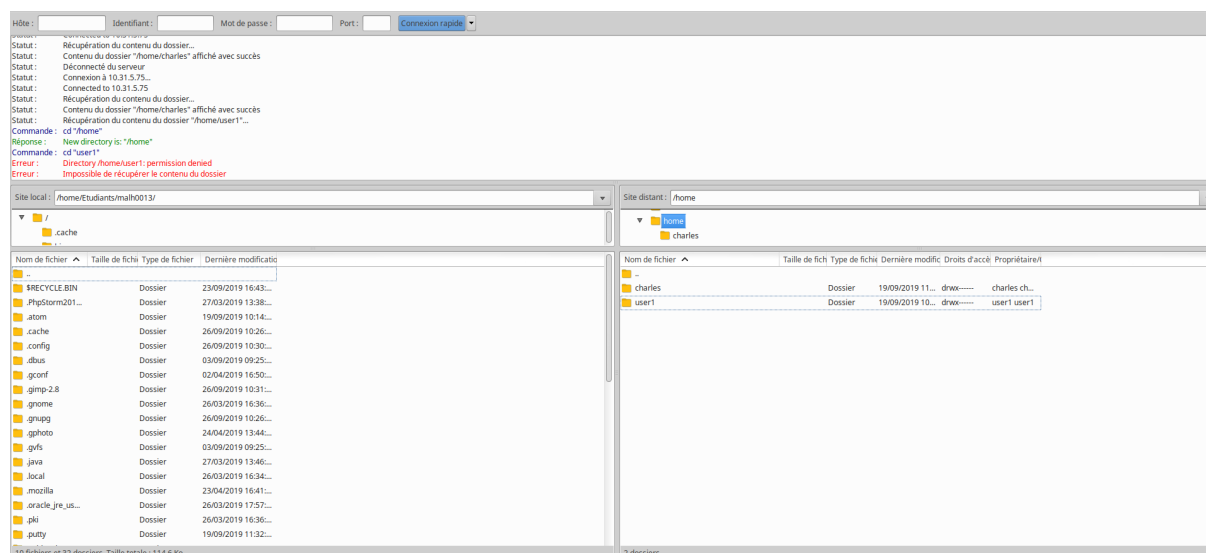


Illustration 12: Tentative de parcours de l'arborescence

```
[root@2a4v1-31uvm75 private]# openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
Generating a 1024 bit RSA private key
.....+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:Reims
Organization Name (eg, company) [Default Company Ltd]:URCA
Organizational Unit Name (eg, section) []:INFO
Common Name (eg, your name or your server's hostname) []:10.31.5.75
Email Address []:charles.malherbe@etudiant.univ-reims.fr
[root@2a4v1-31uvm75 private]# ls
vsftpd.pem
```

Illustration 13: Génération d'un certificat SSL

```
GNU nano 2.3.1 Fichier : vsftpd.conf

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES

rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem

ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Illustration 14: Ajout des lignes à la configuration de vsftpd



Que spécifient les quatre dernières lignes de la configuration ?

<u>ssl_enable=YES</u>	Active SSL
<u>allow_anon_ssl=NO</u>	Interdit aux utilisateurs anonyme d'utiliser SSL
<u>force_local_data_ssl=YES</u>	Oblige les utilisateurs non anonyme à utiliser une connexion SSL pour envoyer des données
<u>force_local_logins_ssl=YES</u>	Oblige les utilisateurs non anonyme à utiliser une connexion SSL pour envoyer les identifiants de connexion

Redémarrer vsftpd et tester la connexion sécurisée

```
Statut : Le port sélectionné est habituellement utilisé par un autre protocole.
Statut : Connexion à 10.31.5.75:22...
Statut : Connexion établie, attente du message d'accueil...
Réponse : SSH-2.0-OpenSSH_6.6.1
Erreur : Impossible d'établir une connexion FTP à un serveur SFTP. Sélectionnez le protocole approprié.
Erreur : Erreur critique : Impossible d'établir une connexion au serveur
```

Illustration 15: Tentative de connexion FTP au serveur (échec)

```
Statut : Connexion à 10.31.5.75...
Statut : Connected to 10.31.5.75
Statut : Récupération du contenu du dossier...
Statut : Listing directory /home/charles
Statut : Contenu du dossier "/home/charles" affiché avec succès
```

Illustration 16: Tentative de connexion en SFTP au serveur (succès)

## 2) Le serveur Apache

### a) Installation

```
[root@2a4v1-3lvm75 ~]# yum install httpd
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.pasteur.fr
 * extras: ftp.pasteur.fr
 * updates: ftp.pasteur.fr
Résolution des dépendances
--> Lancement de la transaction de test
--> Le paquet httpd.x86_64 0:2.4.6-90.el7.centos sera installé
--> Traitement de la dépendance : httpd-tools = 2.4.6-90.el7.centos pour le paquet : httpd-2.4.6-90.el7.centos.x86_64
--> Traitement de la dépendance : /etc/mime.types pour le paquet : httpd-2.4.6-90.el7.centos.x86_64
--> Traitement de la dépendance : libaprutil-1.so.0()(64bit) pour le paquet : httpd-2.4.6-90.el7.centos.x86_64
--> Traitement de la dépendance : libapr-1.so.0()(64bit) pour le paquet : httpd-2.4.6-90.el7.centos.x86_64
```

Illustration 17: Installation d'Apache sur CentOS

### b) Configuration de base

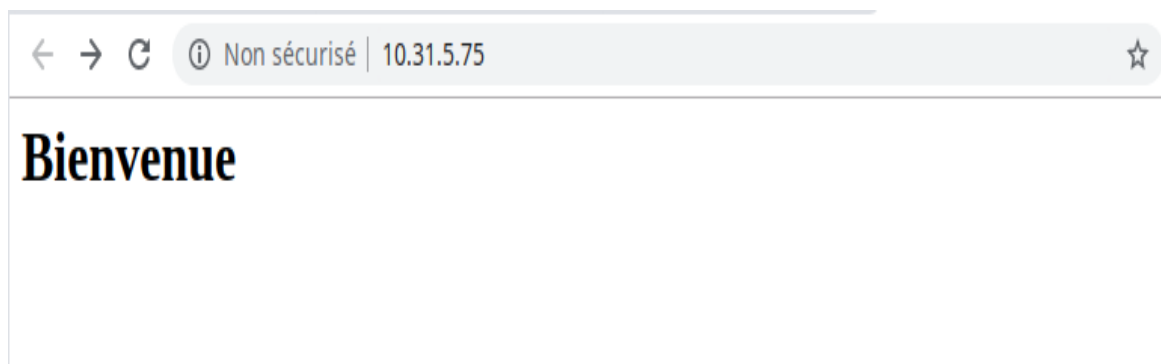
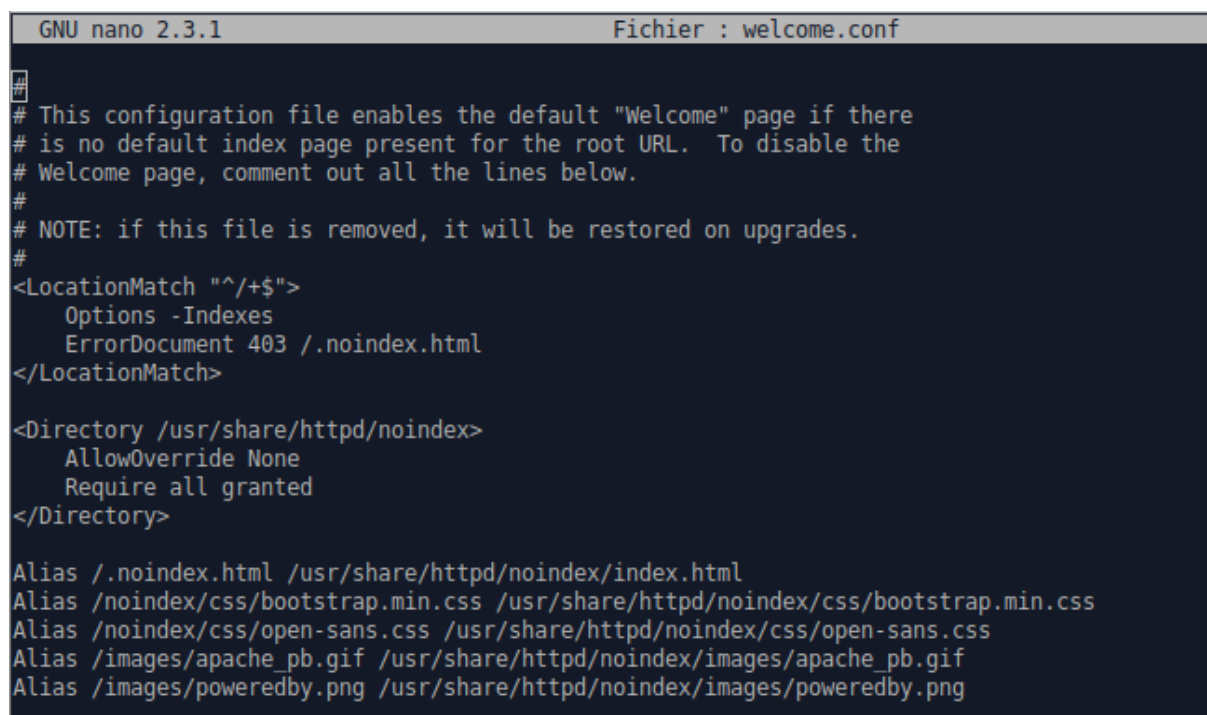


Illustration 18: Page internet de base

Quelles sont les principales instructions de configuration de votre serveur ?

Reproduisez-les sur votre compte-rendu.



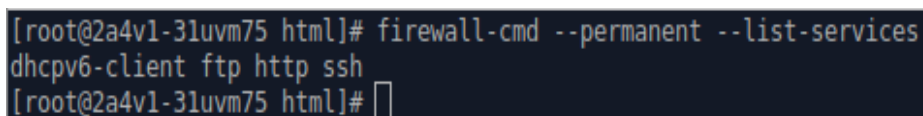
```
GNU nano 2.3.1 Fichier : welcome.conf
#
# This configuration file enables the default "Welcome" page if there
# is no default index page present for the root URL. To disable the
# Welcome page, comment out all the lines below.
#
# NOTE: if this file is removed, it will be restored on upgrades.
#
<LocationMatch "^/+$">
    Options -Indexes
    ErrorDocument 403 /.noindex.html
</LocationMatch>

<Directory /usr/share/httpd/noindex>
    AllowOverride None
    Require all granted
</Directory>

Alias /.noindex.html /usr/share/httpd/noindex/index.html
Alias /noindex/css/bootstrap.min.css /usr/share/httpd/noindex/css/bootstrap.min.css
Alias /noindex/css/open-sans.css /usr/share/httpd/noindex/css/open-sans.css
Alias /images/apache_pb.gif /usr/share/httpd/noindex/images/apache_pb.gif
Alias /images/poweredby.png /usr/share/httpd/noindex/images/poweredby.png
```

Illustration 19: Illustration : principales instructions de configuration du site par défaut

c) Configuration des accès distants autorisés par le pare-feu



```
[root@2a4v1-3lsvm75 html]# firewall-cmd --permanent --list-services
dhcpv6-client ftp http ssh
[root@2a4v1-3lsvm75 html]#
```

Illustration 20: Liste des accès autorisés par le pare feu

## d) Personnalisation du serveur

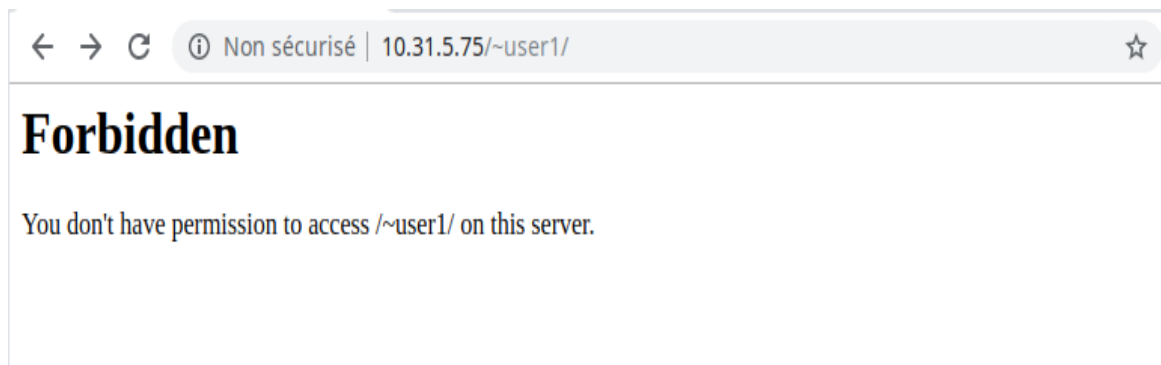


Illustration 21: Index de l'user1 (vide) sans listage des fichiers

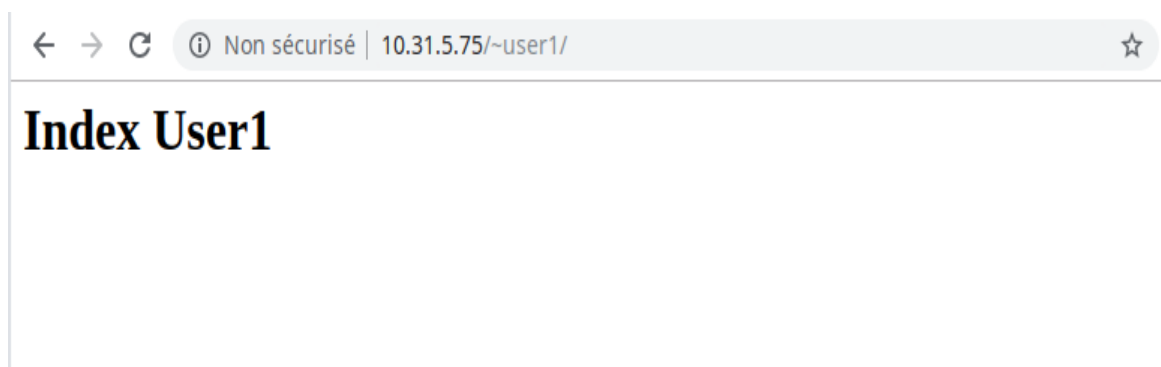


Illustration 22: Index de l'user1

## 3) Telnet et SSH

```
[root@2a4v1-31uvm75 user1]# firewall-cmd --permanent --list-services
dhcpv6-client ftp http ssh telnet
[root@2a4v1-31uvm75 user1]#
```

Illustration 23: Vérification de l'autorisation telnet dans le firewall

### III - Analyse de trafic et sécurité des échanges

#### 1. Pages web personnelles sur le serveur Centos.

```

GNU nano 2.3.1                                Fichier : /var/log/httpd/access_log
10.31.4.136 - - [26/Sep/2019:12:05:26 +0200] "GET /-user1/ HTTP/1.1" 304 - "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:05:26 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "http://10.31.5.75/~user1/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
10.31.4.136 - - [26/Sep/2019:12:05:33 +0200] "GET /-root/ HTTP/1.1" 403 208 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:24 +0200] "GET /-user1/ HTTP/1.1" 304 - "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:55 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:11:56 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:12:27 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:12:27 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:12:28 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:12:28 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:38 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:38 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:39 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:39 +0200] "GET /-user1/ HTTP/1.1" 200 675 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:49 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:49 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:50 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:13:50 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:14:29 +0200] "GET /-user1/ HTTP/1.1" 200 95 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10.31.4.136 - - [26/Sep/2019:12:15:20 +0200] "-" 408 - "-" "-"
10.31.4.84 - - [27/Sep/2019:17:37:49 +0200] "GET / HTTP/1.1" 200 67 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:37:49 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:37:49 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:38:00 +0200] "GET /-user1 HTTP/1.1" 301 233 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:38:00 +0200] "GET /-user1/ HTTP/1.1" 200 95 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:25 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:27 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:27 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:27 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:27 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:27 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.31.4.84 - - [27/Sep/2019:17:47:28 +0200] "GET /-user1/ HTTP/1.1" 403 209 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0"

```

Illustration 24: fichier access\_log de notre serveur (Apache)

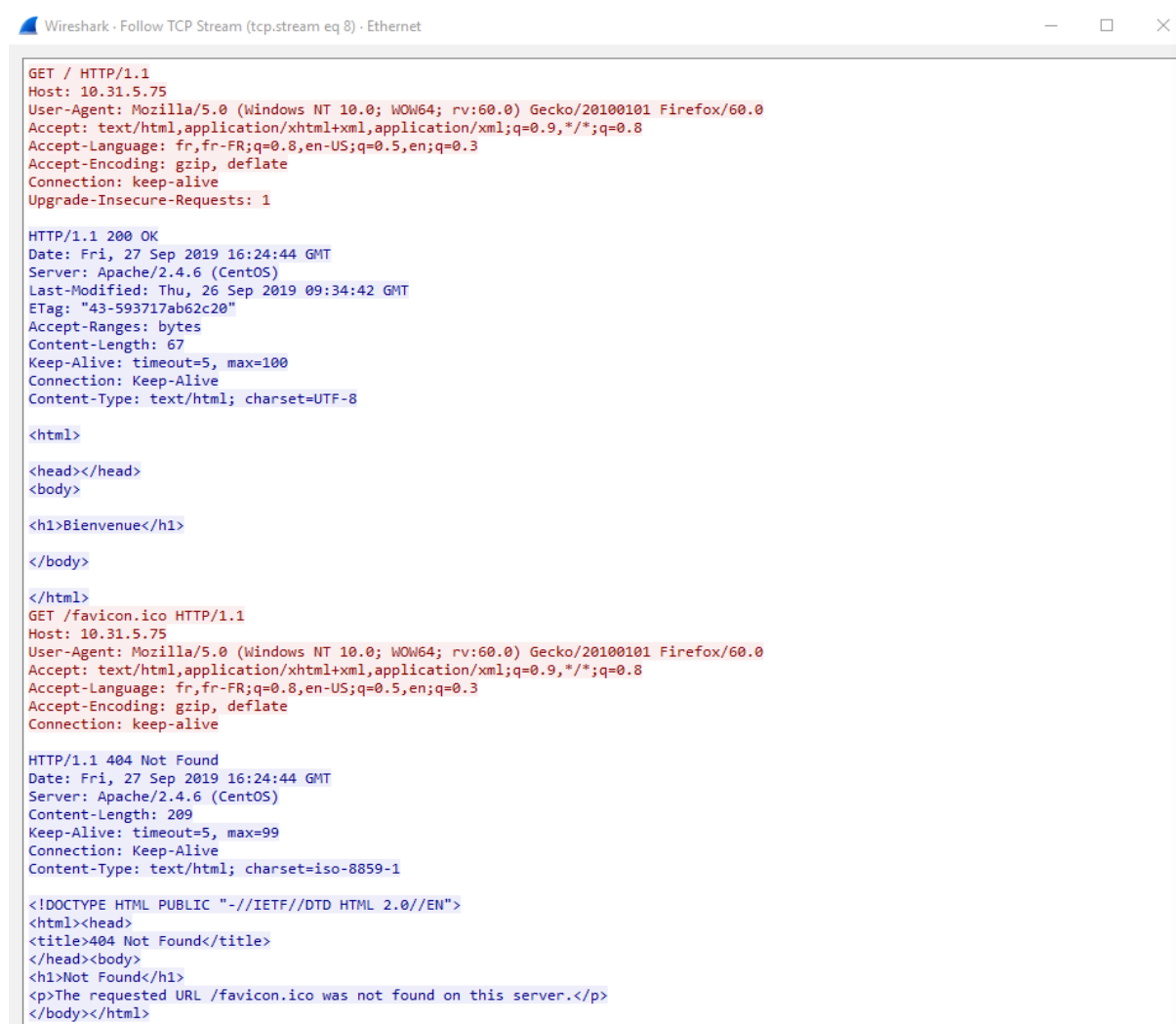
#### Quelles informations du poste client peut-on retrouver à partir du fichier journal des accès ?

Nous avons accès au requête http dans le fichier "/var/log/httpd/access\_log". Elle nous fourni des informations concernant :

- L'adresse IP du client.
- La date et l'heure de réception de la requête.
- La ligne de requête qui inclus la méthode HTTP utilisé (GET ou autres).
- La chemin de la ressource (ici, /-user1).
- La version du protocole client HTTP.
- Le code de statut HTTP que le serveur a envoyé au client (exemple : 404 si ressource introuvable.).
- La taille de la ressource.
- La version du navigateur client (exemple : Mozilla, Chrome, IE...)
- La version du serveur (exemple : Linux...)

## 2. Sécurité des connexions distantes: telnet et ssh

Prendre une capture d'écran montrant ce dialogue.



```

GET / HTTP/1.1
Host: 10.31.5.75
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 27 Sep 2019 16:24:44 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Thu, 26 Sep 2019 09:34:42 GMT
ETag: "43-593717ab62c20"
Accept-Ranges: bytes
Content-Length: 67
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

<head></head>
<body>

<h1>Bienvenue</h1>

</body>

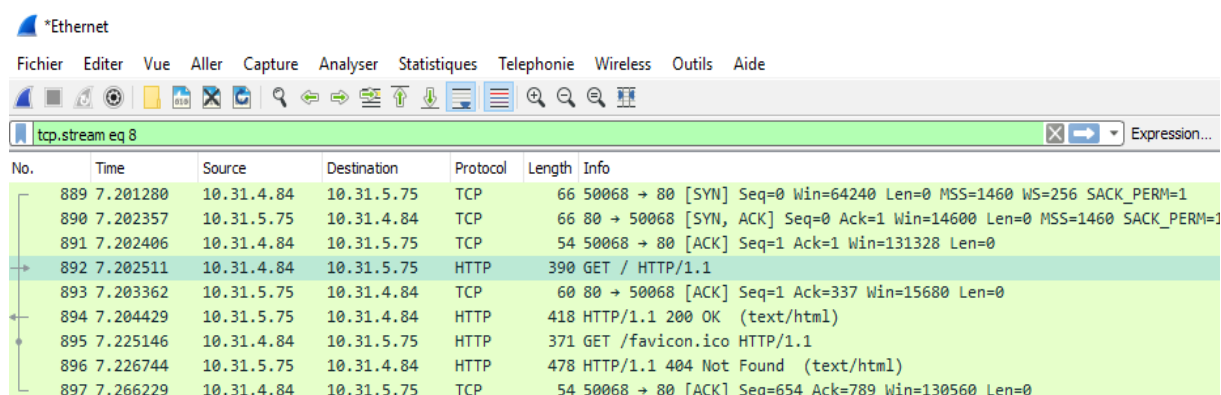
</html>
GET /favicon.ico HTTP/1.1
Host: 10.31.5.75
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 404 Not Found
Date: Fri, 27 Sep 2019 16:24:44 GMT
Server: Apache/2.4.6 (CentOS)
Content-Length: 209
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /favicon.ico was not found on this server.</p>
</body></html>

```

Illustration 25: Flux TCP (HTTP)



\*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

tcp.stream eq 8

No.	Time	Source	Destination	Protocol	Length	Info
889	7.201280	10.31.4.84	10.31.5.75	TCP	66	50068 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
890	7.202357	10.31.5.75	10.31.4.84	TCP	66	80 → 50068 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
891	7.202406	10.31.4.84	10.31.5.75	TCP	54	50068 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
892	7.202511	10.31.4.84	10.31.5.75	HTTP	390	GET / HTTP/1.1
893	7.203362	10.31.5.75	10.31.4.84	TCP	60	80 → 50068 [ACK] Seq=1 Ack=337 Win=15680 Len=0
894	7.204429	10.31.5.75	10.31.4.84	HTTP	418	HTTP/1.1 200 OK (text/html)
895	7.225146	10.31.4.84	10.31.5.75	HTTP	371	GET /favicon.ico HTTP/1.1
896	7.226744	10.31.5.75	10.31.4.84	HTTP	478	HTTP/1.1 404 Not Found (text/html)
897	7.266229	10.31.4.84	10.31.5.75	TCP	54	50068 → 80 [ACK] Seq=654 Ack=789 Win=130560 Len=0

Illustration 26: Échanges HTTP

Noter les informations complémentaires (système d'exploitation, nom des applications...) échangées.

#### CLIENT :

Système d'exploitation : Windows TN 10.0

Nom des applications : Mozilla/5.0

Pour le reste des informations voir Illustration de la page précédente.

#### SERVEUR :

Système d'exploitation : CentOS

Serveur web : Apache 2.4.6

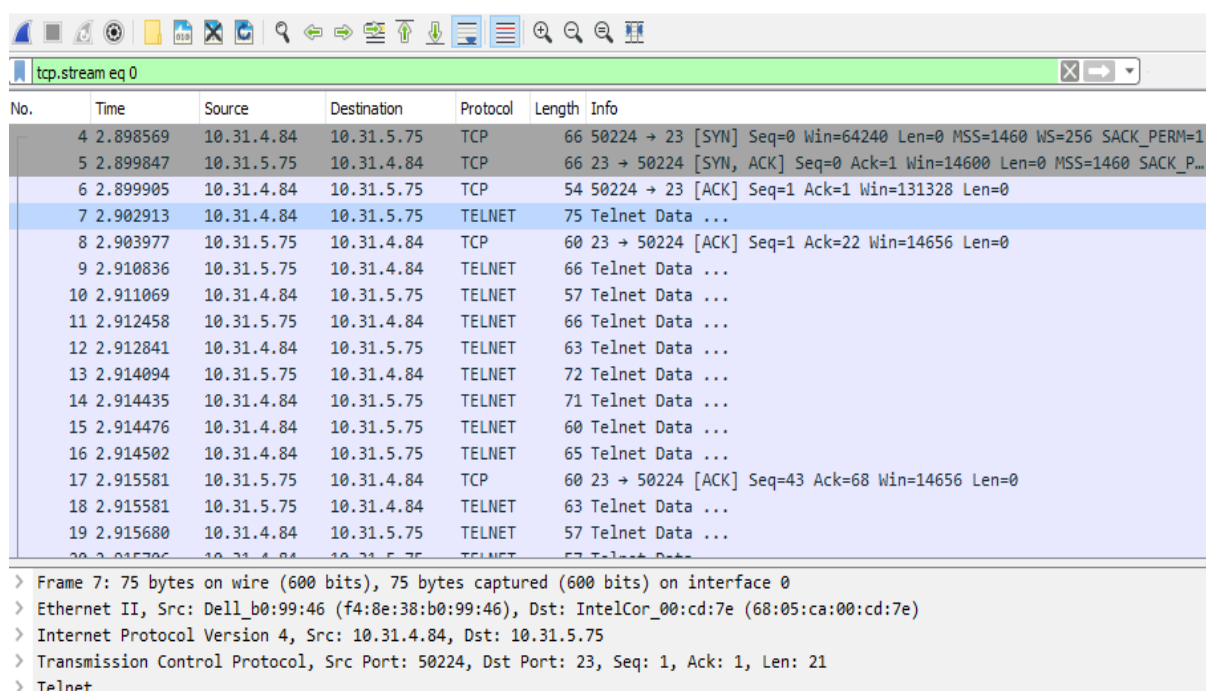
Pour le reste des informations voir Illustration de la page précédente.

#### a) Connexion avec Telnet

Comment s'opère la négociation Telnet entre client et serveur ?

Il semble que la « négociation » Telnet entre client et serveur soit une succession d'échange. (voir illustration ci-dessous)

Noter la succession des trames lors de l'échange.



No.	Time	Source	Destination	Protocol	Length	Info
4	2.898569	10.31.4.84	10.31.5.75	TCP	66	50224 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	2.899847	10.31.5.75	10.31.4.84	TCP	66	23 → 50224 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_P...
6	2.899905	10.31.4.84	10.31.5.75	TCP	54	50224 → 23 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7	2.902913	10.31.4.84	10.31.5.75	TELNET	75	Telnet Data ...
8	2.903977	10.31.5.75	10.31.4.84	TCP	60	23 → 50224 [ACK] Seq=1 Ack=22 Win=14656 Len=0
9	2.910836	10.31.5.75	10.31.4.84	TELNET	66	Telnet Data ...
10	2.911069	10.31.4.84	10.31.5.75	TELNET	57	Telnet Data ...
11	2.912458	10.31.5.75	10.31.4.84	TELNET	66	Telnet Data ...
12	2.912841	10.31.4.84	10.31.5.75	TELNET	63	Telnet Data ...
13	2.914094	10.31.5.75	10.31.4.84	TELNET	72	Telnet Data ...
14	2.914435	10.31.4.84	10.31.5.75	TELNET	71	Telnet Data ...
15	2.914476	10.31.4.84	10.31.5.75	TELNET	60	Telnet Data ...
16	2.914502	10.31.4.84	10.31.5.75	TELNET	65	Telnet Data ...
17	2.915581	10.31.5.75	10.31.4.84	TCP	60	23 → 50224 [ACK] Seq=43 Ack=68 Win=14656 Len=0
18	2.915581	10.31.5.75	10.31.4.84	TELNET	63	Telnet Data ...
19	2.915680	10.31.4.84	10.31.5.75	TELNET	57	Telnet Data ...

> Frame 7: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0  
 > Ethernet II, Src: Dell\_b0:99:46 (f4:8e:38:b0:99:46), Dst: IntelCor\_00:cd:7e (68:05:ca:00:cd:7e)  
 > Internet Protocol Version 4, Src: 10.31.4.84, Dst: 10.31.5.75  
 > Transmission Control Protocol, Src Port: 50224, Dst Port: 23, Seq: 1, Ack: 1, Len: 21  
 > Telnet

Illustration 27: Échanges Telnet

Pouvez-vous retrouver le login et le mot de passe dans les trames échangées ?

Oui, la preuve en image :

```

.....'.....'..#..'..#.....P.....'.....'.....38400,38400.....'.....XTERM.....!.....!
Kernel 3.10.0-229.14.1.el7.x86_64 on an x86_64
2a4v1-31uvm75 login: uusseerr11

Password: iutinfo

Last login: Fri Sep 27 18:41:39 from pc054.iut-rcc-info.urca
.]0;user1@2a4v1-31uvm75:~.[?1034h[user1@2a4v1-31uvm75 ~]$

```

Illustration 28: Flux TCP (Telnet)

b) Connexion en SSH

Comment se déroule la communication ?

No.	Time	Source	Destination	Protocol	Length	Info
4	5.875225	10.31.4.84	10.31.5.75	TCP	66	50389 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	5.876520	10.31.5.75	10.31.4.84	TCP	66	22 → 50389 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_P...
6	5.876647	10.31.4.84	10.31.5.75	TCP	54	50389 → 22 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7	5.885139	10.31.4.84	10.31.5.75	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.71)
8	5.886239	10.31.5.75	10.31.4.84	TCP	60	22 → 50389 [ACK] Seq=1 Ack=29 Win=14656 Len=0
9	5.888876	10.31.5.75	10.31.4.84	SSHv2	77	Server: Protocol (SSH-2.0-OpenSSH_6.6.1)
10	5.890780	10.31.5.75	10.31.4.84	TCP	1514	22 → 50389 [ACK] Seq=24 Ack=29 Win=14656 Len=1460 [TCP segment of...]
11	5.890821	10.31.4.84	10.31.5.75	TCP	54	50389 → 22 [ACK] Seq=29 Ack=1484 Win=131328 Len=0
12	5.892054	10.31.5.75	10.31.4.84	SSHv2	234	Server: Key Exchange Init
13	5.892694	10.31.4.84	10.31.5.75	SSHv2	1222	Client: Key Exchange Init
14	5.896702	10.31.4.84	10.31.5.75	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
15	5.897736	10.31.5.75	10.31.4.84	TCP	60	22 → 50389 [ACK] Seq=1664 Ack=1245 Win=17536 Len=0
16	5.913273	10.31.5.75	10.31.4.84	SSHv2	262	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
17	5.922695	10.31.4.84	10.31.5.75	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
18	5.924214	10.31.5.75	10.31.4.84	SSHv2	118	Server: Encrypted packet (len=64)
19	5.975108	10.31.4.84	10.31.5.75	TCP	54	50389 → 22 [ACK] Seq=1325 Ack=1936 Win=130816 Len=0

> Frame 28: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0  
 > Ethernet II, Src: IntelCor\_00:cd:7e (68:05:ca:00:cd:7e), Dst: Dell\_b0:99:46 (f4:8e:38:b0:99:46)  
 > Internet Protocol Version 4, Src: 10.31.5.75, Dst: 10.31.4.84  
 > Transmission Control Protocol, Src Port: 22, Dst Port: 50389, Seq: 2032, Ack: 1517, Len: 96  
 > SSH Protocol

Illustration 29: Échanges SSH



Pouvez-vous retrouver le login et le mot de passe dans les trames échangées ?

Non, la preuve en image :

```

SSH-2.0-PuTTY_Release_0.71
SSH-2.0-OpenSSH_6.6.1
...d
....bN.....(n..3....curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-
exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1...'ssh-rsa,ecdsa-sha2-
nistp256,ssh-ed25519....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-
gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-
cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....hmac-
md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-
sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-
sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-
sha1-96,hmac-md5-96....hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-
sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-
etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....none,zlib@openssh.com....none,zlib@openssh.com.....w.`T,
%.6$.!.....curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,rsa2048-sha256,rsa1024-
sha1,diffie-hellman-group1-sha1...'ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-
dss....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.com,
3des-ctr,3des-cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-
ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.com,3des-ctr,3des-cbc,blowfish-ctr,blowfish-
cbc,arcfour256,arcfour128....hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-
etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-etm@openssh.com....hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-
etm@openssh.com....none,zlib@openssh.com....VR.....j..E.G..R..oE.H..Y
.pw.....a.T...(.none,zlib@openssh.com....9].V).g...NH7c...~.2+;.....n.I..{7.t.a.X3k..._.....S....ssh-
ed25519...@,Q...$.F...h...I...%.F...).i...4.....l.....F
.....\K..
..
.....
.....
.D.....E..H.
.....P.....J.....h.G.Z.[w/.$Z.....A.M4.-t.?L.L.8q,...@.....~...`...e...Q@0....(EX.0k.....3.9...7.w...$.S.v...a.'42c;
j...x...n./...5<.Q9W.t.8..9'$j.T.....t.=2.\...k...y.....9.6.TjvS9M.D
.e(;.0...@Z?...?...../N...n.x:...>PZV....dL...X...P...Ma...[...~cb.n.8..3.n...@|.....gVQ..3[Rj]...|...K.3..|1Y..
\qL...a....W-({rQ.....h..E.!(.u....y...Y5.)K....\Dw[Uz...Z..[Wq.R...->).....q.*u.....+
...
u\...
...Z...f?
Z...m.t.i.[.R....G...o.QM..5c.wY....5*...L.`~..^.....a0..4.S=nD|}wJ%.\ ]..n..TW"S.....xMc....kD!.Ht...L...
\H$.h...M)....%.v...5{H6.s.y...0+. ....R..)....._=s..u...0...m.NL..\..!.....(...Dh5....=zdZ.....R..2...
.-?...9D..EP.....EG.o... F7..JfX.M&k.....c.!G.55E..Y.p..i.GRD..~^/[.....&tG...:2.#.`r.H...>#.U....*..!
0..._U...?...5[.Z.k.H..D.XA....90rT...v.....I;..LA.Z?|.....$Z.W.e...T..d...:bN.-.a.N.w...e.o....WnbX.m.....
(.V.D.).k'f..3...d{.U..0@...yr./).%.p...l[.y1....T...:zY;.....=...A.f.Q.....'
7.....3.0)...L((...QcKMB...'..YF..""A.....).5.B,...?.....l.$uP..#...r]>.@?U.I.....Z.]#.....E.....
\].p.....m.e.b?(.....^.....Co..5....V..4...a/Y..a=...o.U...[J.N=Q.....):C.....}j="..Z.0..~I10.4u.V.]...K..e}
(d3.IU...Q4..R...+J...6.X..(+.7..r...R.p.+Xw0.9...A.....msaH...`.Sh.)...kS.H..$.Bg..|
8..L.M.n.T.^.....L..u..B..OF.Xq.Tv"...n'~...}....dv.....0..S...>xI.....Tw`...iA.g.....;.....I$It.X.q....TvF.
\....._Z.kB...Ch.e~9.....0.v

```

Illustration 30: Flux TCP (SSH)