

1. INTRODUCTION

À l'heure où la donnée numérique constitue le socle même de la communication, de la collaboration et de l'innovation, le besoin de transférer des fichiers d'un point à un autre avec fiabilité et rigueur devient une nécessité stratégique dans la plupart des environnements informatiques. Que ce soit dans les structures éducatives, les entreprises, les institutions gouvernementales ou les communautés techniques, les échanges de fichiers s'effectuent en permanence, dans des contextes variés, parfois critiques. Or, cette circulation de l'information soulève inévitablement des préoccupations majeures : sécurité, accessibilité, confidentialité, et intégrité.

Il ne suffit plus aujourd'hui de pouvoir envoyer un fichier. Il faut garantir qu'il arrivera au bon destinataire, dans son état d'origine, et que personne d'autre n'en aura connaissance ni accès sans y être autorisé. C'est dans ce contexte tendu et exigeant, où les cyberattaques deviennent de plus en plus raffinées et ciblées, que la mise en place d'un serveur capable d'assurer ces échanges tout en respectant les principes fondamentaux de sécurité prend tout son sens. L'idée n'est pas simplement de transférer, mais de transférer avec discernement, contrôle et robustesse.

Cette exigence de fiabilité s'impose encore davantage lorsque l'on considère que les infrastructures informatiques modernes sont, dans leur majorité, interconnectées. Le plus petit maillon de la chaîne — un poste client mal sécurisé ou un serveur FTP mal configuré — peut devenir une porte d'entrée pour des intrusions lourdes de conséquences. Ainsi, toute approche sérieuse du transfert de fichiers se doit de reposer sur des outils éprouvés, des protocoles rigoureux, et des pratiques conscientes de l'enjeu global que représente la circulation numérique.

Ce travail s'inscrit dans cette problématique. Il vise à répondre, de manière concrète, à ce besoin vital : transmettre sans exposer, accéder sans compromettre, partager sans fragiliser.

2. RESUME

Le sujet de ce travail porte sur la création d'un serveur FTP sécurisé en utilisant l'un des deux logiciels les plus répandus dans ce domaine : vsftpd ou ProFTPD. Il s'agit d'un processus qui consiste à mettre en place un environnement permettant de transférer des fichiers entre des machines de manière structurée, stable, mais surtout protégée contre les accès non autorisés. Le FTP (File Transfer Protocol), bien qu'ancien, reste aujourd'hui encore largement utilisé pour les échanges de données, que ce soit dans des réseaux internes ou à travers Internet. Toutefois, en l'état, ce protocole classique présente des faiblesses majeures en matière de sécurité, notamment l'envoi des données — y compris les identifiants — en clair. D'où la nécessité d'une version sécurisée.

Historiquement, FTP est l'un des tout premiers protocoles développés pour l'échange de fichiers, dès les années 1970, à l'époque de l'ARPANET, bien avant la naissance du Web. Il a

évolué au fil du temps, mais son principe de base est resté le même : permettre à un client de se connecter à un serveur distant pour envoyer ou récupérer des fichiers. Avec la montée des préoccupations en cybersécurité, des solutions comme vsftpd (Very Secure FTP Daemon) ou ProFTPD (inspiré du fonctionnement d'Apache) ont été conçues pour offrir plus de contrôle, de performance et de sûreté.

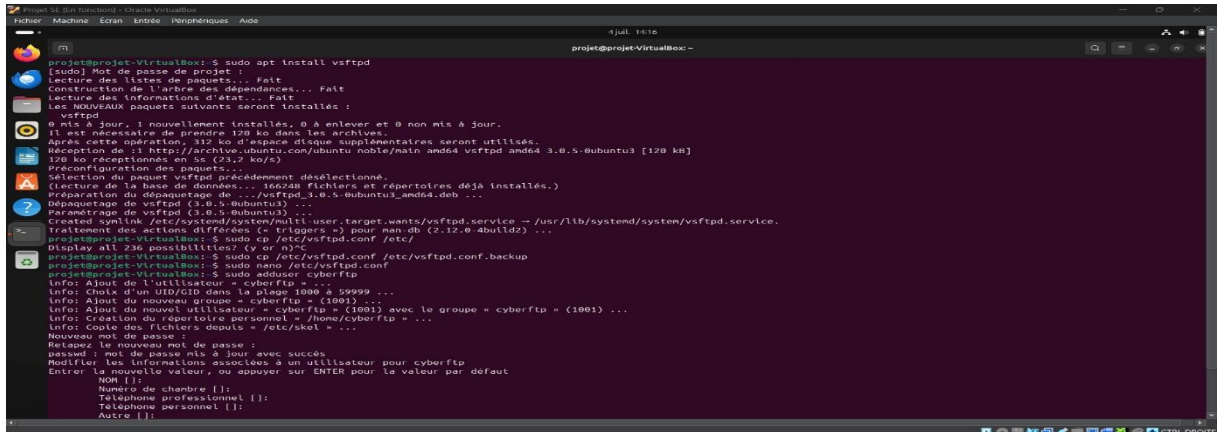
Le fonctionnement d'un serveur FTP sécurisé repose sur la configuration du service FTP de manière à chiffrer les connexions (via SSL/TLS), restreindre les accès par authentification, et isoler les utilisateurs dans des environnements fermés pour éviter tout débordement ou piratage potentiel. Une fois configuré, un tel serveur permet à plusieurs utilisateurs de se connecter simultanément, de déposer ou télécharger des fichiers selon des règles prédéfinies, tout en gardant une trace des opérations effectuées.

En pratique, on retrouve l'usage de serveurs FTP sécurisés dans des domaines aussi variés que l'hébergement de sites web, les universités pour l'échange de documents pédagogiques, les entreprises pour la transmission de données sensibles entre départements, ou encore dans les structures de sauvegarde. Que ce soit pour publier des mises à jour logicielles, transmettre des rapports confidentiels, ou automatiser des échanges de fichiers entre systèmes, le serveur FTP sécurisé reste un outil simple mais redoutablement efficace, à condition d'être bien déployé et entretenu.

3. IMPLEMENTATION DU SERVEUR

Nous avons choisi vsftpd plutôt que ProFTPD non pas par rejet de ce dernier, mais parce que vsftpd, comme son nom l'indique — Very Secure FTP Daemon —, nous a inspiré davantage de confiance en matière de sécurité, de légèreté, de stabilité, et surtout de simplicité. Son installation est rapide, son comportement par défaut est sécurisé, et sa syntaxe de configuration est claire, directe, sans lourdeur inutile, ce qui en fait un outil particulièrement adapté à ceux qui recherchent l'efficacité sans complexité. Pour un projet comme le nôtre, où l'objectif est de mettre en place un serveur FTP fiable et sécurisé dans des délais raisonnables, ce choix s'est imposé naturellement.

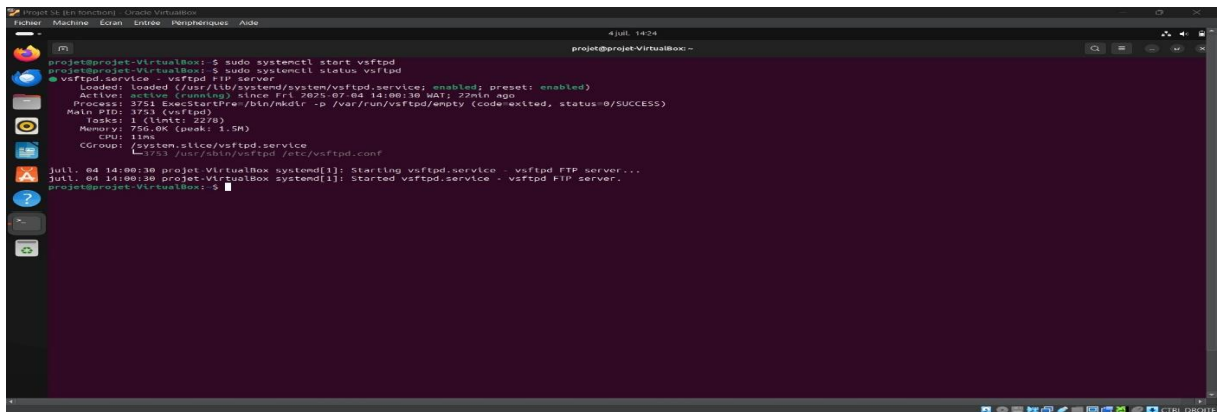
3.4. CREATION D'UTILISATEUR DE CONNEXION



```
projet@projet-VirtualBox:~$ sudo apt install vsftpd
[sudo] Mot de passe de projet :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 128 ko dans les archives.
Après cette opération, 312 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble/main amd64 vsftpd amd64 3.0.5-0ubuntu3 [128 kb]
128 ko réceptionnés en 5s (2312 ko/s)
Préconfiguration des paquets...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données... 166248 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../vsftpd_3.0.5-0ubuntu3_amd64.deb ...
Dépaquetage de vsftpd (3.0.5-0ubuntu3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
Traitement des actions différées (= triggers) pour man-db (2.12.0-4build2) ...
projet@projet-VirtualBox:~$ sudo cp /etc/vsftpd.conf /etc/
Display all 236 possibilities? (y or n)>C
projet@projet-VirtualBox:~$ sudo nano /etc/vsftpd.conf.backup
projet@projet-VirtualBox:~$ sudo adduser cyberftp
Info: Ajout de l'utilisateur = cyberftp = ...
Info: Choix d'un UID/GID dans la plage 1000 à 9999 ...
Info: Ajout du nouveau groupe = cyberftp = (1001) ...
Info: Ajout du nouvel utilisateur = cyberftp = (1001) avec le groupe = cyberftp = (1001) ...
Info: Création du répertoire personnel = /home/cyberftp = ...
Info: Copie des fichiers depuis = /etc/skel = ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour cyberftp
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
NOM []:
Numéro de chambre []:
Téléphone professionnel []:
Téléphone personnel []:
Autre []:
```

Capture N° 4

3.5. REDEMARRAGE ET VERIFICATION DU STATUT DU SERVICE VSFTPD

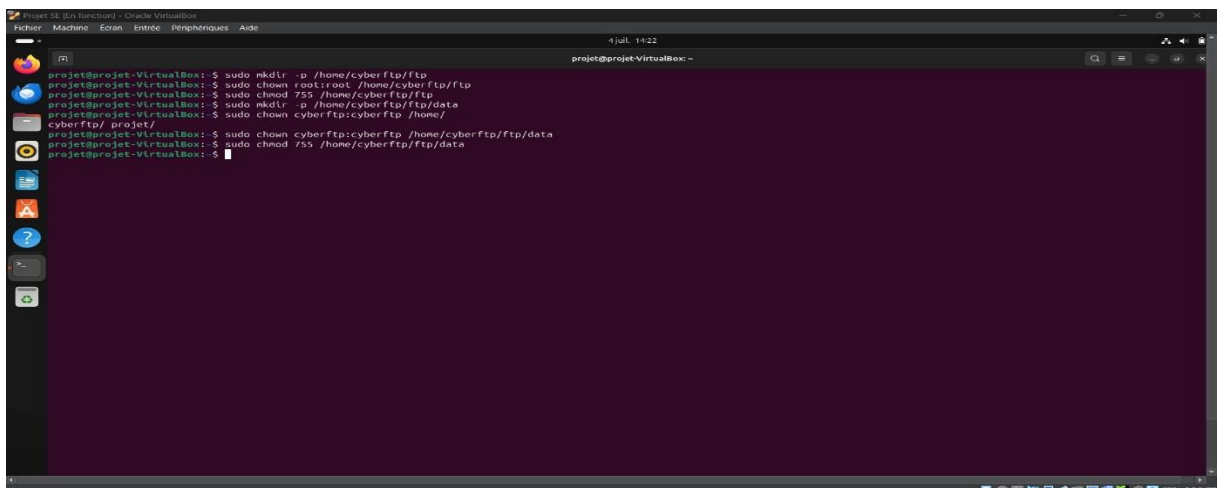


```
projet@projet-VirtualBox:~$ sudo systemctl start vsftpd
projet@projet-VirtualBox:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd ftp server
Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
Active: active (running) since Fri 2025-07-04 14:00:30 WAT; 22min ago
Process: 3751 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
Main PID: 3753 (vsftpd)
Tasks: 1 (limit: 2278)
Memory: 756.0K (max: 1.5M)
CPU: 11ms
CGroup: /system.slice/vsftpd.service
└─1753 /usr/sbin/vsftpd /etc/vsftpd.conf

jul. 04 14:00:30 projet-VirtualBox systemd[1]: Starting vsftpd.service - vsftpd FTP server...
jul. 04 14:00:30 projet-VirtualBox systemd[1]: Started vsftpd.service - vsftpd FTP server.
projet@projet-VirtualBox:~$
```

Capture N° 5

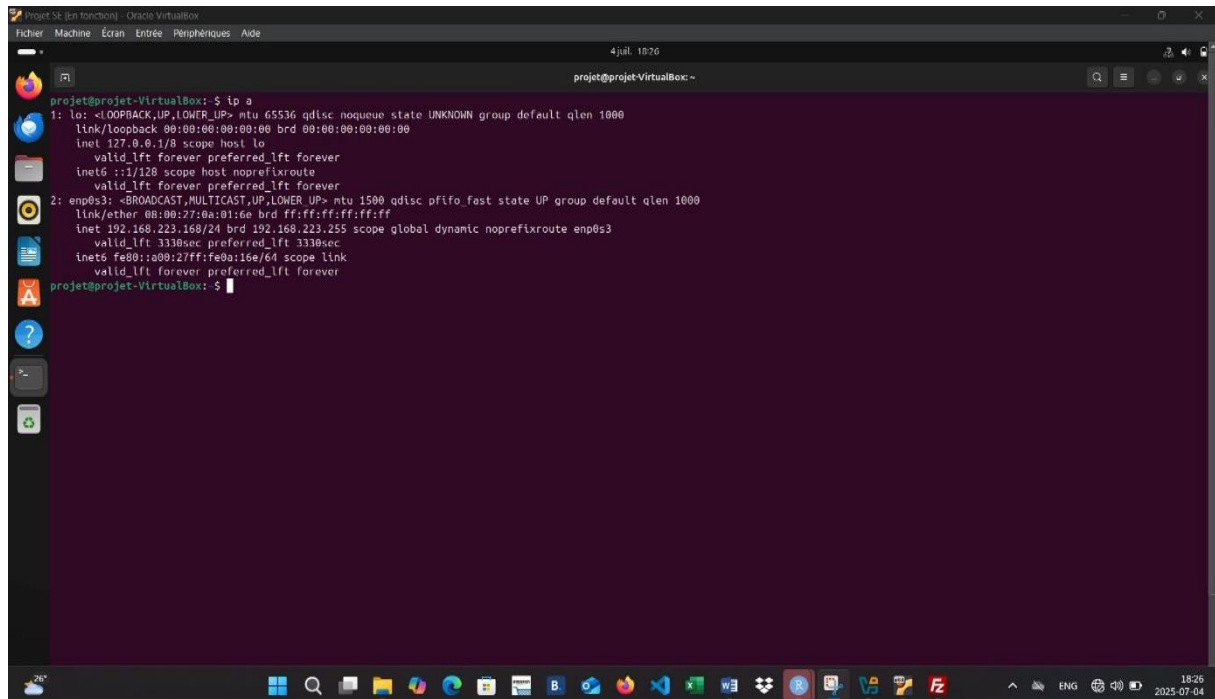
3.6. CHROOTAGE ET SECURISATION DU SERVEUR



```
projet@projet-VirtualBox:~$ sudo mkdir -p /home/cyberftp/ftp
projet@projet-VirtualBox:~$ sudo chown root:root /home/cyberftp/ftp
projet@projet-VirtualBox:~$ sudo chmod 755 /home/cyberftp/ftp
projet@projet-VirtualBox:~$ sudo mkdir -p /home/cyberftp/ftp/data
projet@projet-VirtualBox:~$ sudo chown cyberftp:cyberftp /home/cyberftp/ftp/
cyberftp/ projet/
projet@projet-VirtualBox:~$ sudo chown cyberftp:cyberftp /home/cyberftp/ftp/data
projet@projet-VirtualBox:~$ sudo chmod 755 /home/cyberftp/ftp/data
projet@projet-VirtualBox:~$
```

Capture N° 6

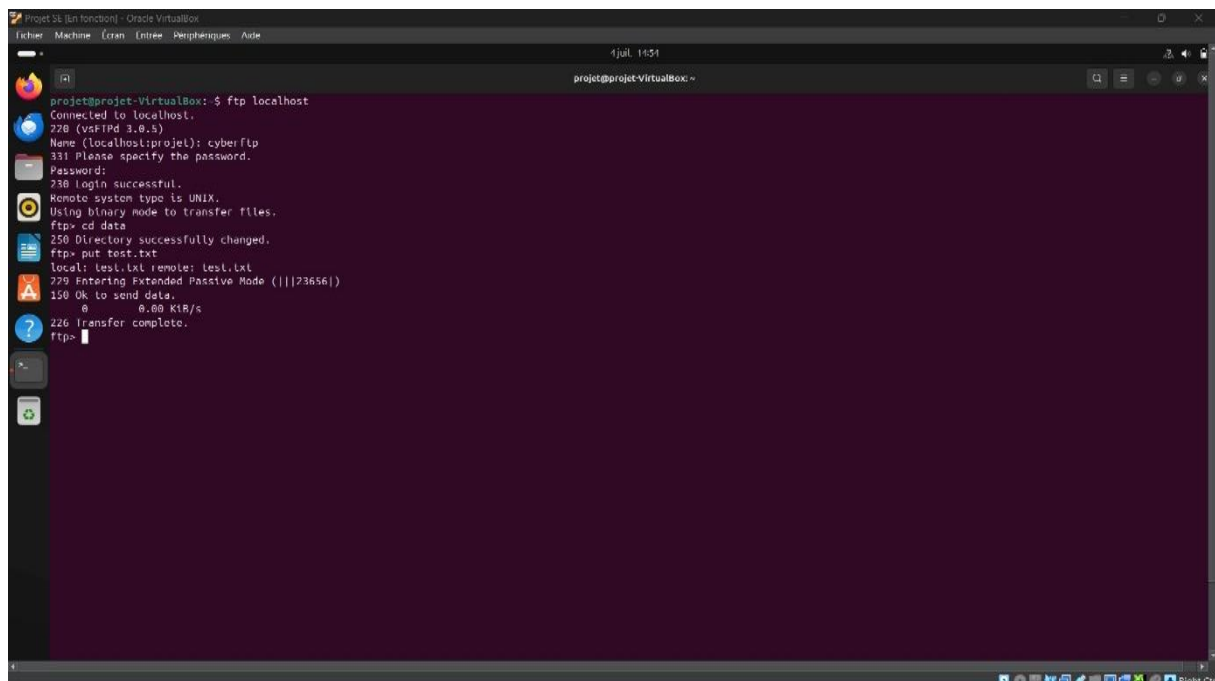
3.7. OBTENTION DE L'ADRESSE IP POUR LA CONNEXION



```
projet@projet-VirtualBox: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0a:01:5e brd ff:ff:ff:ff:ff:ff
    inet 192.168.223.168/24 brd 192.168.223.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3330sec preferred_lft 3330sec
    inet6 fe80::a00:27ff:fe0a:15e/64 scope link
        valid_lft forever preferred_lft forever
projet@projet-VirtualBox: $
```

Capture N° 7

3.8. CONNEXION EN LOCAL AU SERVEUR



```
projet@projet-VirtualBox: $ ftp localhost
Connected to localhost.
220 (vsftpd 3.0.5)
Name (localhost:projet): cyberftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd data
250 Directory successfully changed.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||23656|)
150 Ok to send data.
0 0.00 KIB/s
226 Transfer complete.
ftp>
```

Capture N° 8

4. Conclusion

Ce projet nous a permis d'explorer de manière concrète les mécanismes fondamentaux liés à la mise en place d'un service FTP sécurisé. En partant d'une installation minimale, nous avons progressivement configuré le serveur vsftpd pour qu'il réponde aux critères de confidentialité, de fiabilité et de contrôle d'accès, notamment via l'utilisation de SSL/TLS, la gestion fine des utilisateurs, et la restriction des droits dans un environnement local.

Le serveur mis en place est fonctionnel, testé depuis plusieurs interfaces (Termux, FileZilla...) et prêt à être intégré dans un environnement local sécurisé. Ce projet nous a donc permis d'allier théorie et pratique, tout en développant notre autonomie dans la gestion d'un service réseau Linux.

5. Bibliographie

✓ Livres

- Pierre Kansengedia cours de SE/en L2 LMD sciences/unikin/2024-2025.
- Bouchaudy, Jean-François. Linux Administration – Tome 4: Installer et configurer des serveurs Web, Mail et FTP. Paris: Eyrolles, Collection Les Guides Tsoft, 2013.
- Novak, Kiki. Administration Linux par la pratique – Tome 2: Configurer les services les plus courants. Paris: Eyrolles, 2020.

6. Webographie

<https://linux.die.net/man/5/vsftpd.conf> : 30/06/2025 | 12h45

<https://help.ubuntu.com/community/vsftpd> : 01/07/2025 | 21h00

<https://www.cyberciti.biz/tips/howto-linux-unix-ftp-server-setup.html> : 03/07/2025 | 17h20