Administration et sécurité des réseaux

Chapitre 3, Partie 3

Le Protocole FTP
(File Transfer Protocol)

Plan

- Présentation du protocole
- Fonctionnement
- Configuration et options

Présentation de FTP

- **Fonctionnalités :**
  - Téléchargement (Download) anonyme ou par utilisateur.
  - Dépôt (Upload) anonyme ou par utilisateur
-
- **Deux types d'accès FTP:**
  - **Utilisateur** (l'utilisateur requiert un compte sur le serveur)
  - **Anonyme**: n'importe qui sur l'Internet peut initier une connexion FTP:
    - Login: « anonymous »
    - Password: n'importe quel MdP est accepté
    - Défini par défaut dans chaque serveur FTP, il a accès au répertoire /var/ftp comme racine.
    - Il peut avoir le droit de Download ou Upload.
    - Utile pour des connexions rapides anonymes et sans authentification (à travers Internet par exemple).

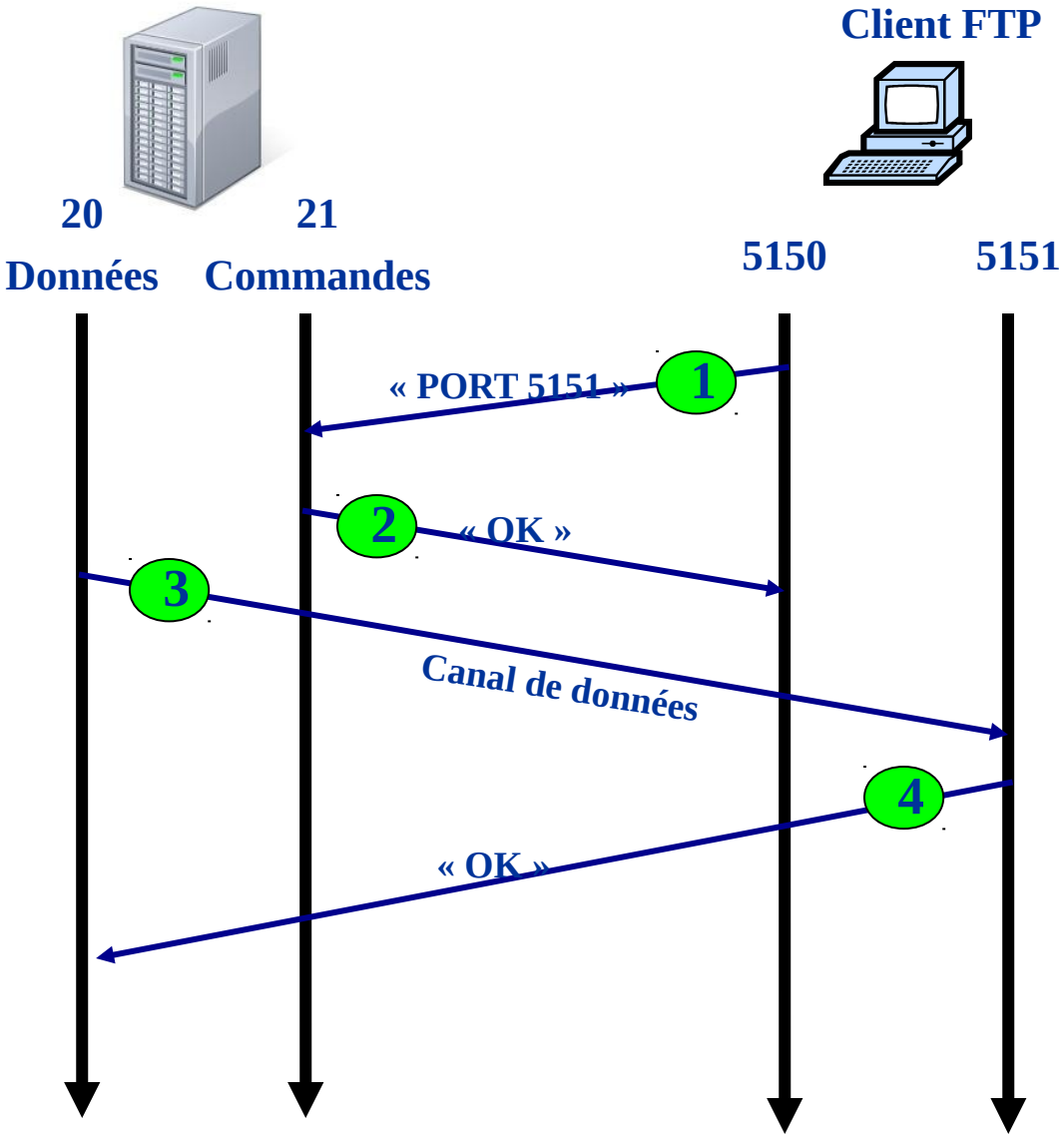
Présentation de FTP

- **FTP utilise deux connexions TCP séparées:**
  - **Canal de Commandes:** pour transporter les commandes et leurs résultats entre le client et le serveur
  - **Canal de données:** pour transporter les listes de répertoires et les fichiers transférés.

- **Deux modes de connexions FTP:**
  - **Normal**
  - **Passif**

FTP en mode normal

1. Le client ouvre un canal de commande vers le serveur et lui donne le second n° de port.
2. Le serveur acquitte.
3. Le serveur ouvre un canal de données vers le second port du client.
4. Le client acquitte.



FTP en mode passif

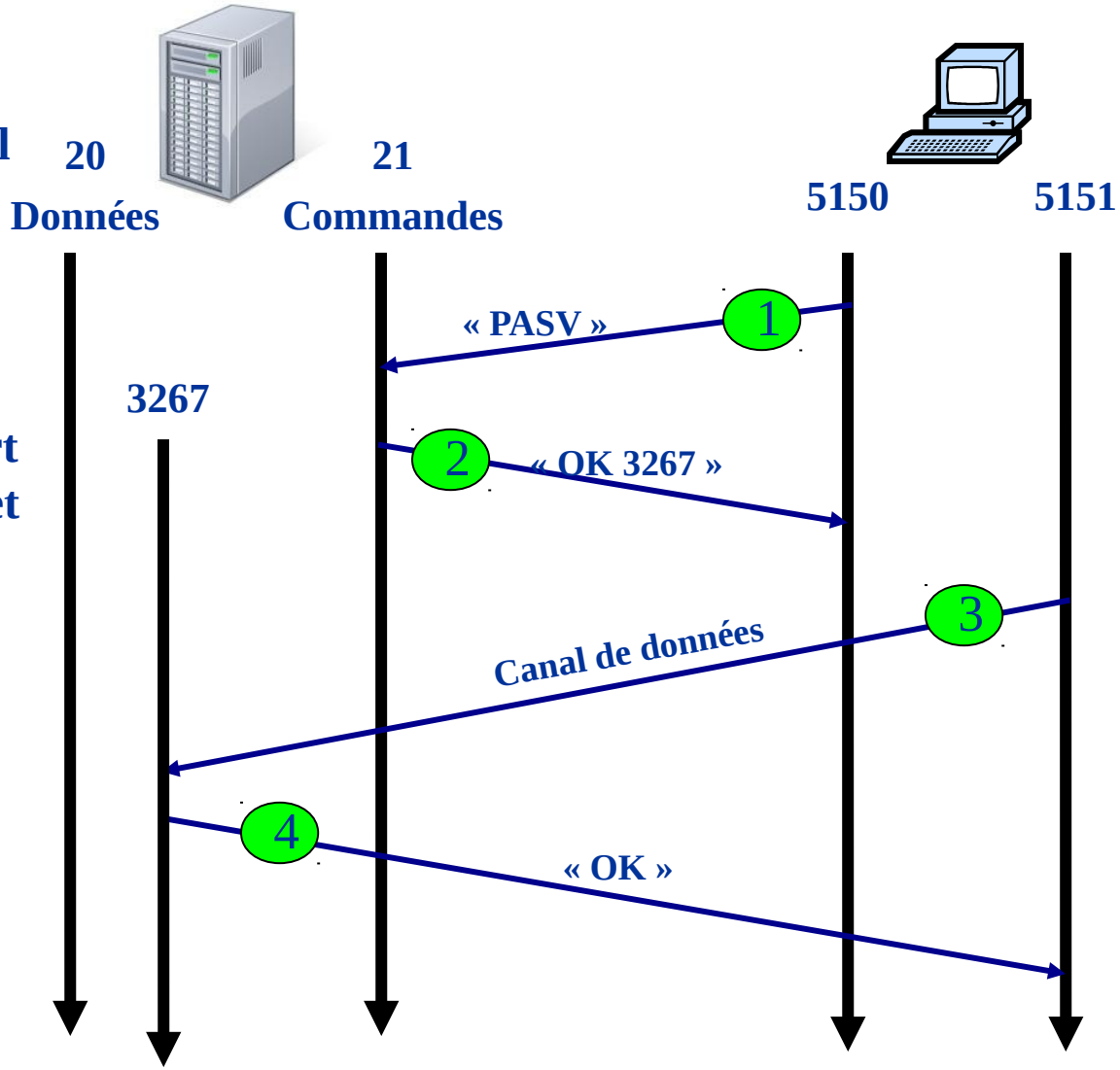
- Supporté par la plupart des serveurs et des clients FTP

1. **Le client ouvre un canal de commandes vers le serveur et lui précise le mode passif.**

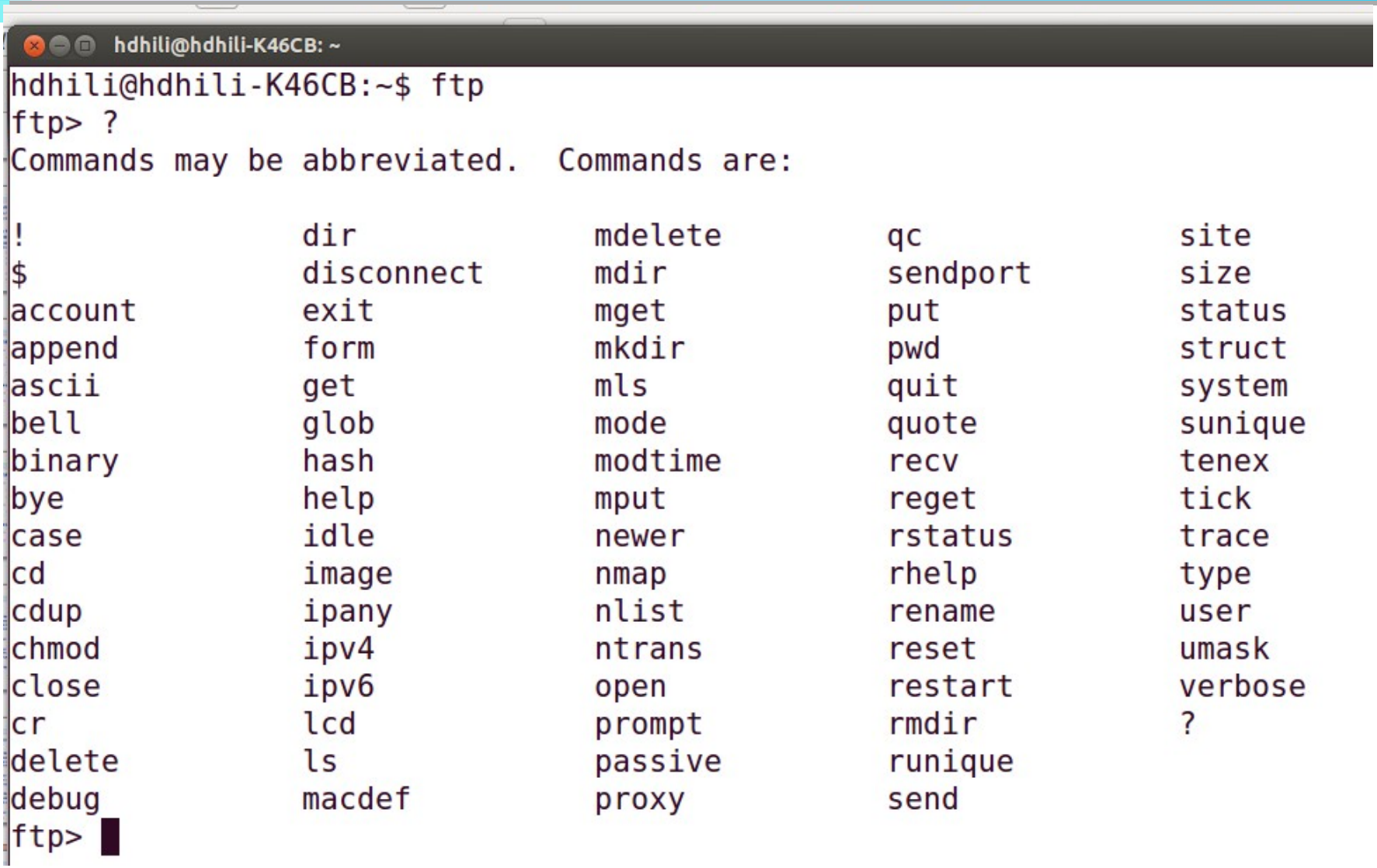
2. **Le serveur alloue le port pour le canal de données et en informe le client.**

3. **Le client ouvre le canal de données vers le second port du serveur.**

4. **Le serveur acquitte.**



Commandes FTP



Service FTP sous Linux

- Implémentation courante du serveur sous linux : **vsftpd**
- Identité :
  - Type : service standalone
  - Ports : 20 et 21
  - Démon : /etc/init.d/vsftpd (service vsftpd start)
  - Fichier de configuration : /etc/vsftpd.conf
  - Logs : /var/log/messages , /var/log/vsftpd.log et /var/log/xferlog(si activé)

Service FTP: mise en oeuvre

- Configuration à travers le fichier /etc/vsftpd.conf
- Configuration du service de téléchargement (Download).
  - Pour autoriser la connexion par le compte anonymous :

    anonymous_enable=YES
  - Pour autoriser la connexion par les utilisateurs non privilégiés du système et ne les autoriser que de travailler dans leur répertoire sous /home

    local_enable=YES

    chroot_local_user=YES
- Configuration du service de dépôt (Upload) anonyme.
  - Pour autoriser l'écriture dans les répertoires par défaut :

    write_enable=YES
  - Pour autoriser le dépôt (Upload) par l'utilisateur anonymous :

    anon_upload_enable=YES
  - Créer un répertoire sous /var/ftp réservé pour le Upload
  - Lui assigner les permissions nécessaires pour qu'il soit accessible pour l'utilisateur anonymous
- A chaque modifications des paramètres du service relancer vsftpd :

  service vsftpd restart Ou /etc/init.d/vsftpd restart

Service FTP: mise en oeuvre

- Connexion d'un client à un serveur FTP:
  - **ftp : Commande en mode texte interactif existante sous plusieurs systèmes d'exploitations.**
    - Commandes disponibles sous ftp : ls, get, put, cd, lcd, pwd, ? , bye
  - **À travers un navigateur web (ftp://@ipftpserver)**
  - **Plusieurs applications graphiques selon les distributions**
    - Exemple : Filezilla
      - Full-featured graphical FTP/FTPS/SFTP client
      - Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)

FTPS: FTP over SSL/TLS

Créer un certificat et une clé privée pour le serveur

sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc/ssl/private/ssl-cert-snakeoil.key -out /etc/ssl/certs/ssl-cert-snakeoil.pem

Ajouter sur vsftpd.conf

location of the RSA certificate to use for SSL encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

location of the RSA key to use for SSL encrypted connections.
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

force SSL. This will restrict clients that can't deal with TLS
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

FTPS: FTP over SSL/TLS

configure the server to use TLS (more secure than SSL)

#explicitly allowing TLS and denying the use of SSL

ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

#If set to yes, all SSL data connections are required to exhibit SSL session reuse (which proves that they know the same master secret as the control channel). Although this is a secure default, it may break many FTP clients, so you may want to disable it
require_ssl_reuse=NO

#select which SSL ciphers vsftpd will allow for encrypted SSL connections
ssl_ciphers=HIGH

allow writeable chroot if **chroot_local_user** was set to **YES**
allow_writeable_chroot=YES

À faire en TP