Cyber-Sécurité
TD8 - 2023

Concepts d'architecture (Partitions, MBR, ...)

TD individuel
« La connaissance s'acquiert par l'expérience, tout le reste n'est que de l'information.»
Albert Einstein

- **Modalité de réalisation du TD**

- **Documents et liens pour la réalisation du TD :**
  - **Python :**
    - Document Python officiel :https://docs.python.org/fr/3/
    - Document Python Fonction officiel : https://docs.python.org/3/library/functions.html
    - Index des bibliothèques officielles Python : https://docs.python.org/3/py-modindex.html
    - Communauté officielle Python : https://www.python.org/community/
  - **Jupiter-Lab :**
    - **Ensemble des exercices de ce TD devra être réaliser avec Jupiter-lab**
  - Installation de Jupyter-Lab : https://jupyter.org/install
  - Documentation de Jupiter-lab : https://docs.jupyter.org/en/latest/
  - Utilisation de Jupiterlab pour le champ **Markdown** :
    - https://jupyterlab.readthedocs.io/en/stable/user/file_formats.html
  - **Modalité de Réalisation du TD :**
    - **Document d'audit avec explication de vos recherches**
    - **fonctions Python de l'ensemble des exercices**
    - **Vous devez préparer une présentation pour expliquer l'ensemble des solutions que vous proposer pour réaliser ces exercices**
  - **Modalité de remise du TD :**
    - Votre .zip contiendra obligatoirement :
      - L'ensemble des fonctions Python dans **jupyter-lab au format « ipynb »**
        - Votre ipynb devra contenir obligatoirement:
          - Votre nom et prénom, N° du TD, N°de l'exercice
          - Question et réponse à l'exercice
          - Code Python, une fonction par cellule avec commentaires
          - ...
    - **Rappel des commandes pour Jupiter-lab**
      - le « **!** » permet de lancer une commande
        - par exemple : !ping 8.8.8.8 (dns de google)
        - *le « # » pour les commentaires*

1 Exercice – Données personnelles

1.1 Exo1_1 : Données personnelles :

- Avec l'explosion des technologies de l'information et des communications, toutes les activités humaines peuvent être étroitement liées à la collecte et au traitement de données personnelles. Aujourd'hui, les frontières entre le monde réel et le monde virtuel ou numérique sont de plus en plus étroites. La numérisation de la société ne cesse de s'accélérer et transforme profondément nos manières de vivre, d'envisager nos relations, de nous comporter ou de travailler. Cette évolution comporte certes de nombreux avantages mais aussi est porteuse de risques
  - Répondre aux questions suivantes :
    - Qu'est-ce qu'une donnée personnelle ? (donner des exemples)
    - Que sont les données sensibles ? (donner des exemples)
    - Qu'est-ce que les métadonnées ? (donner des exemples)
    - Qu'est-ce que le cyberespace ?
    - Pourquoi les données personnelles passionnent tant ? donner votre avis.
    - Internet, est-il un cimetière de données personnelles ?
    - Si je n'utilise pas ou très peu Internet, suis-je concerné par la sécurité des données personnelles ? Pourquoi ?
    - Le « sentiment de sécurité dans le cloud», donner votre avis.
    - « Pas grave si on prend mes données, je n'ai rien à cacher », donner votre avis.

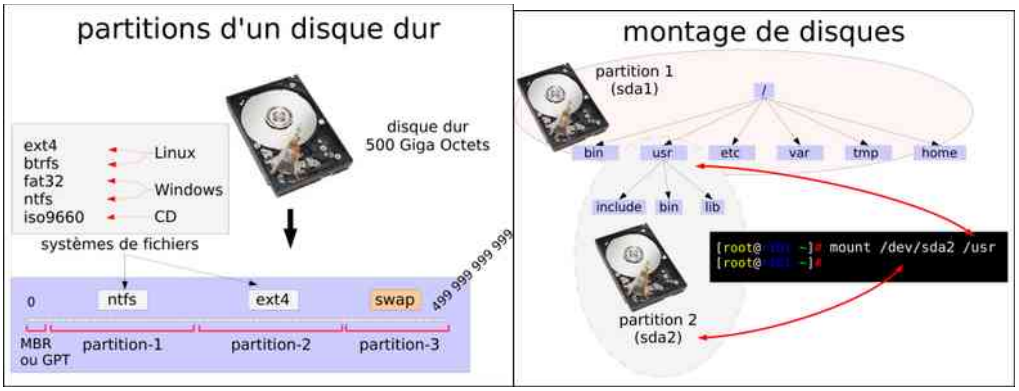
1.2

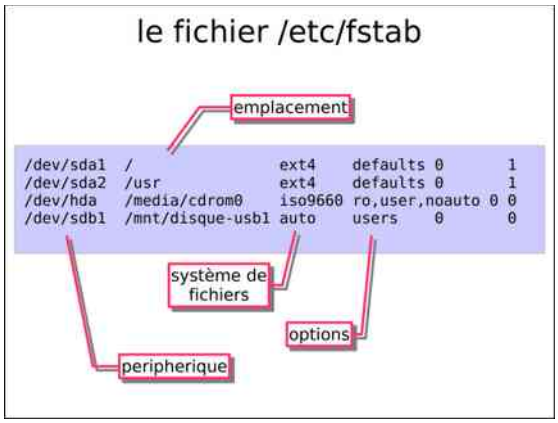
2 Exercices – Disque / USB /

Préparation de la clé USB pour les exercices suivant :

- Suivez les manipulations avec votre enseignant :
  - Taille 34MO
  - Nom Tfat16 ou Tfat32
  - **lsblk | grep -Ev 'loop|sr0'**
  - **cfdisk**

Dans les exercices suivantes nous allons manipuler des disques, des partitions et des systèmes de fichiers.





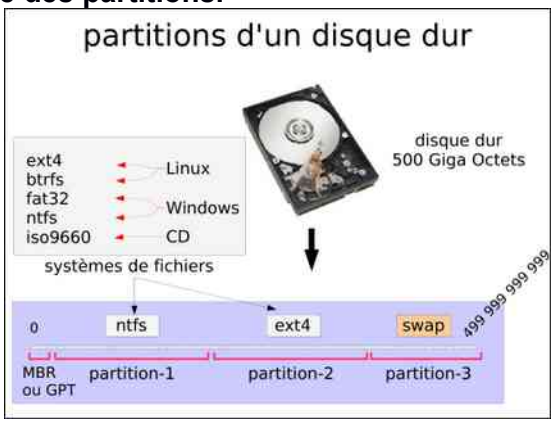
2.1 Exo2_1 : "df" est un programme en mode ligne de commande

- **Quelle est la commande permettant d'afficher la quantité d'espace libre restant sur les différents disques montés sur le système?**
- **Sur votre ordinateur, quel est le périphérique associé au répertoire racine du système de fichiers ?**

2.2 Exo2_2 : Valider le périphérique associé au répertoire racine du système de fichiers avec la commande : « lsblk | grep -Ev 'loop|sr0'» ou « df -x squashfs »

- Rechercher le périphérique de votre clé USB : si vous n'êtes pas sur retirer la clé usb et refaite la commande, remettez la clé et refaite la commande la clé.

2.3 Exo2_3 : "fdisk" est un programme en mode ligne de commande qui permet de manipuler la table des partitions.



- La table des partitions se trouve au tout début du disque (MBR ou GPT). Elle définit, entre autres, le début et la fin de chaque partition.

- Attention: la table des partitions se trouve sur le disque de la partition principale par exemple /dev/sda et pas sur une partition secondaire comme /dev/sda1.

- Lancez la commande "**sudo fdisk « avec le périphérique de votre disque dur»** " sûrement /dev.sda
  - Appuyez sur la touche "m" pour lister les différentes options possibles.
  - **"fdisk" n'écrit rien sur le MBR ou GPT tant que vous n'utilisez pas la commande "w". N'hésitez donc pas à expérimenter: en quittant ("q") vous abandonnez tous vos changements.**
  - Afficher la table des partitions
  - Combien de partitions est-ce qu'il y a actuellement sur votre disque?
  - Il est fortement possible que vous ayez une partition pour le "swap" :
    - lorsque votre ordinateur n'a pas assez de mémoire vive, il utilise cette partition comme un "prolongement" de sa mémoire.
    - Dans un ordinateur, opération fréquente consistant à vider une portion moins utilisée des données situées en mémoire (page) et à la stoker sur le disque temporairement, permettant à d'autres données d'être traitées pendant ce temps.
    - Cette opération ralentie le traitement des données, mais permet de disposer d'une mémoire de traitement supérieure à la mémoire réellement disponible : la mémoire virtuelle.
    - Quitter « fdisk » avec la commande « q **»**

2.4 Exo2_4 : Création d'une partition avec la commande "fdisk" sur votre clé USB

- **ATTENTION : vérifier que le Devices est bien la clé USB avec la commande : «lsblk | grep -Ev 'loop|sr0'» ou «df -x squashfs» ou «*df -H* »**
- **La commande lsblk récupère des informations détaillées sur les périphériques de bloc, telles que vos disques durs, vos lecteurs flash et leurs partitions.**
  - pour ma part le nom du Device de la clé USB est /dev/sdc
    - rappel "fdisk" n'écrit rien sur le MBR tant que vous n'utilisez pas la commande "w".
    - Avec la commande de fdisk, donner la commande pour vérifier la place disponible sur votre clé USB, normalement vous remarquerez qu'il reste beaucoup de place libre (non partitionné) sur votre clé USB.
    - **Attention au manip suivantes:**
      - dans fdisk taper la commande « i » pour information
      - vérifier que c'est bien la clé USB
      - Création de la 1er Partition de 2Go:
        - Exécutez le n commande pour créer une nouvelle partition.
          - Primary partition
          - Sélectionnez le numéro de partition en saisissant le numéro par défaut (2).
          - Après cela, on vous demande le secteur de début valider la valeur par défaut .
          - La dernière invite est liée à la taille de la partition. Vous pouvez choisir d'avoir plusieurs secteurs ou de définir la taille en mégaoctets ou gigaoctets. Taper +2G pour définir la taille de la partition sur 2 Go.
          - Enfin saisir i pour avoir l'information de la partition nouvellement créer .
          - Un message apparaît confirmant que la partition est créée.

      - Création de la 2éme Partition de +2Go sur votre clé USB
    - Une fois que vous êtes 100% surs de vous, écrivez votre table de partions sur le disque avec "w".

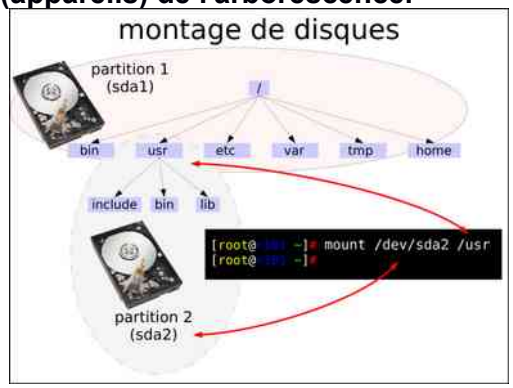
- Sortie de la commande « fdisk »
- **Vous venez de créer deux partitions sur votre clé USB.** Pour l'instant elles ne contiennent rien : c'est juste une série d'octets disponibles.
- Tapez "sudo fdisk -l" pour obtenir une liste des partitions des périphériques branchés.

2.5 Exo 2_5 :Création d'un système de fichiers

- Vous venez de créer deux partitions. Pour l'instant elles ne contiennent rien : c'est juste une série d'octets disponibles.
- Tapez "**sudo fdisk -l** " pour obtenir une liste des partitions des périphériques branchés. Pour valider les créations des partitions sur votre clé USB.
- Nous allons maintenant créer un système de fichiers on utilise la commande :
  - "mkfs -t ext4 nom-périphérique"
  - par exemple : **sudo mkfs -L "Text4" -t ext4 /dev/sdc2**
    - dans le cas ou vous avez ce message :
      - mount: /dev/sdbc2: Aucun fichier ou dossier de ce type
      - faire la commande : umount /dev/sdc2
- formater en ntfs la 3eme partition avec la commande :
  - **sudo mkfs.ntfs -L "Tntfs" /dev/sdc3**
    - **si c'était en Fat32 :** mkfs.vfat /dev/sdc3

2.6 Exo 2_6 : Monter et démonter des médias sous Linux

- Tous les fichiers d'un **système de fichiers Linux** sont organisés sous la forme d'une grande arborescence ayant comme racine ' **/** '.
- Ces fichiers peuvent être répartis sur différents périphériques en fonction de votre table de partition, initialement votre répertoire parent est monté (c'est-à-dire attaché) à cet arbre à ' **/** ', d'autres peuvent être montés manuellement à l'aide de l'interface graphique (si disponible) ou à l'aide **de la commande mount** .
- **La commande mount** est utilisée pour monter le système de fichiers trouvé sur un périphérique sur la structure arborescente (**système de fichiers Linux**) enracinée à ' **/** '.
- **La commande umount Inversement, peut être utilisée pour détacher les périphériques (appareils) de l'arborescence.**



- **Utilisation de la commande "mount"**
  - Pour l'instant nous avons:
    - crée une partition
    - crée un système de fichiers sur la partition
    - Pour pouvoir utiliser notre système de fichiers, il faut l'associer à un répertoire.

2.7 Exo 2_7 : Suivez l'ensemble des recommandations pour comprendre le fonctionnement du chargement par mount .

- **Créer la partition de +2Go au nom de label : Tntfs**
- **lancer les commandes suivantes :**

- la commande "**sudo mkfs.ntfs -L "Tntfs"**
- vérifiez que **que la clé USB** n'est pas encore associé à un répertoire.

- Lancer la commande : *mount | column -t*
- Créez un répertoire essai-mount dans /media (/media existe déjà)
- Créez un fichier Test18 dans /media/essai-mount et vérifiez qu'il existe
- Ensuite, sortez de ce répertoire par la commande « cd ».

- Utiliser la commande « mount » pour associer le périphérique au répertoire /media/essai-mount .
- Vérifier si votre fichier existe toujours dans le répertoire /media/essai-mount
- Créer un autre fichier Test21.txt dans le répertoire

- Lancer la commande : pour démonter la clé USB :
  - umount /media/essai-mount
  - Vérifier le contenu du répertoire /media/
  - Que remarquez-vous ?

3 Exercices – Disque / Gparted

3.1 Exo3_1 :Test de Chiffrement de partition : à faire avec votre enseignant.

3.2 Exo3_2 :Gparted Documentation :

- https://gparted.org/display-doc.php%3Fname%3Dhelp-manual

3.3 Exo3_3 : Sauvegarder la partition cryptée en fichier

- **utiliser ce programme pour la sauvegarde https://doc.ubuntu-fr.org/tutoriel/comment_sauvegarder_partition_avec_partimage**
- **Rechercher la commande en ligne de commande pour sauvegarder une seule partition en .iso.**

3.4 .

4 Challenge :

4.1 Exo4-1 : Challenge 1 : créer un programme python qui trouve le password du pdf qui est sur DVO

4.2 Exo4-2 : Challenge 2 : créer un programme python qui trouve la paraphrase de votre partition cryptée

5 Complément d'informations : Outils Linux et MBR / GPT

5.1 **Exo5_1 :** Outils linux **Inxi** et **hdparm** :

- La commande **« Inxi »** est un script bash de 10 000 lignes qui récupère les détails du matériel à partir de plusieurs sources et commandes différentes sur le système et génère un rapport facile à lire.
- La commande « **hdparm** » est utilisée pour afficher et exécuter les opérations du lecteur de disque, y compris la gestion de l'alimentation, les paramètres DMA et les paramètres matériels.
- Installation des packages : sudo apt install inxi - sudo apt install hdparm
- Lancer la commande : inxi -Fx
- Lancer la commande : sudo hdparm -I /dev/sdX
  - https://linuxhint.com/linux-hdparm-command-tutorial/

5.2 Exo5_2 : **Intérêt de la transformation MBR2GPT :** L'une des caractéristiques les plus inhabituelles de gdisk est sa capacité à lire une table de partition MBR ou une

étiquette de disque BSD et la convertir au format GPT sans endommager le contenu des partitions sur le disque. Cette fonctionnalité existe pour permettre la mise à niveau vers GPT en cas de limitations des MBR ou BSD les labels de disque deviennent trop onéreux - par exemple, si vous souhaitez ajouter d'autres systèmes d'exploitation à une configuration multi-boot, Certains systèmes d'exploitation que vous souhaitez ajouter nécessitent également de nombreuses partitions principales pour tenir sur un disque MBR. (Malheureusement, beaucoup ces systèmes d'exploitation ne peuvent pas gérer GPT.).

- Commandes :
  - **liste des devices : lsblk | grep -Ev 'loop|sr0'**
  - **sudo gdisk /dev/sdX**
- Les utilisateurs de fdisk reconnaîtront bon nombre de ces commandes, telles que : m, d , n et p .
- Par exemple,
  - (m) pour afficher les commandes
  - (p) pour afficher la table de partition du disque et vérifier que vous travaillez sur le disque sur lequel vous pensez travailler,
- **Transformation MBR en GPT avec la commande : gdisk /dev/sdXXX (p,o,p)**
  - **pour enlever certaines limites :**
    - **https://www.rodsbooks.com/gdisk/walkthrough.html**
    - **https://www.rodsbooks.com/gdisk/mbr2gpt.html**
    - **https://linuxconfig.org/how-to-manipulate-gpt-partition-tables-with-gdisk-and-sgdisk-on-linux**

5.3 Attention avec les manipulations de votre clé, lisez bien le document avant de vous lancer, dans un mbr2gpt ou inversement