Initiation
à
UNIX / LINUX

☞ Il s’agit d’un système d’exploitation.

Programme gérant :

- ➢ Le dialogue homme-machine
- ➢ Les ressources matérielles internes : unité centrale, disque dur, mémoire centrale,…
- ➢ Les périphériques : lecteurs USB, de dvd, imprimante,…
- ➢ L’exécution des programmes applicatifs
- ➢ La communication avec le monde extérieur

Exemples de systèmes d’exploitation :

- ➢ Unix, Windows XX, Mac OS, …

Organisation d’Unix





Matériel

Noyau

Shell

X-window





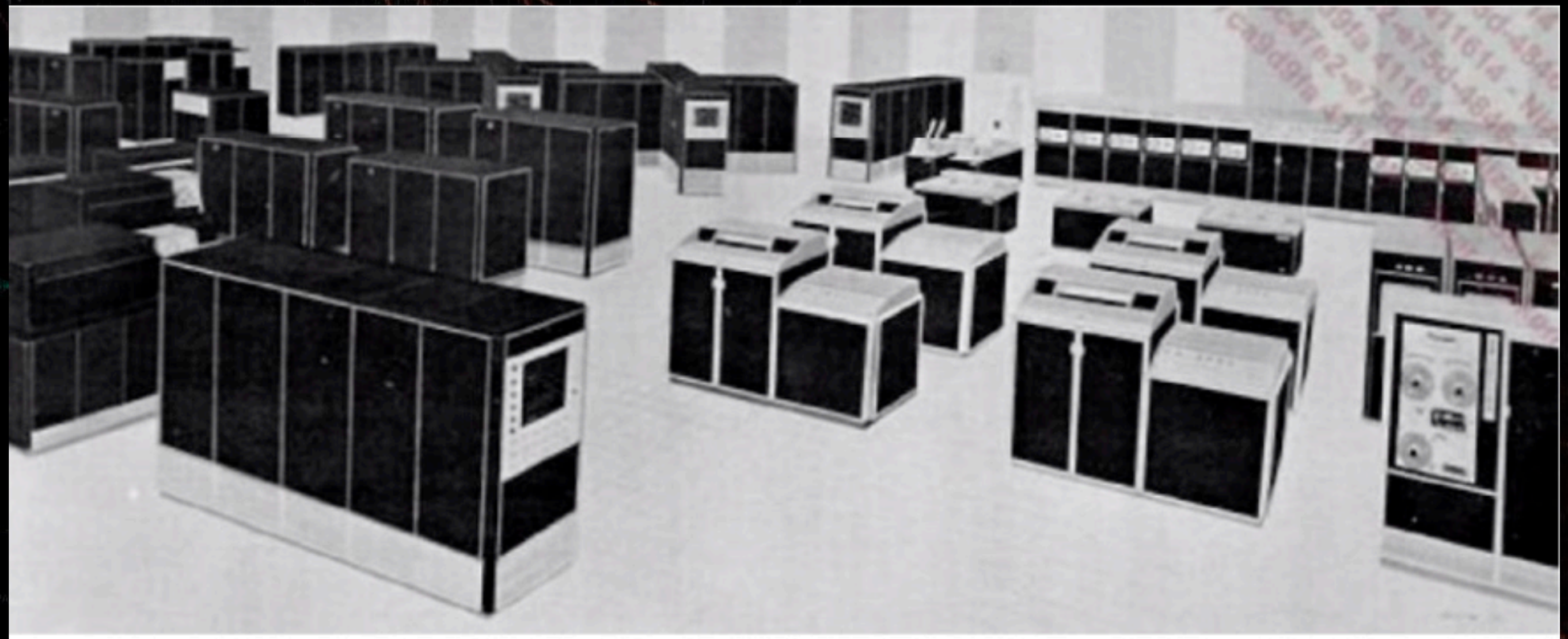
Caractéristiques d’Unix

- Multi-utilisateurs
  - Connexion de plusieurs utilisateurs sur la même machine simultanément
- Multi-tâches
  - Traitement simultanée de plusieurs tâches avec protection de la mémoire
- Sécurisé

  Protection des données :
  - Du système vis à vis des utilisateurs
  - Des utilisateurs entre eux

Origine d’Unix

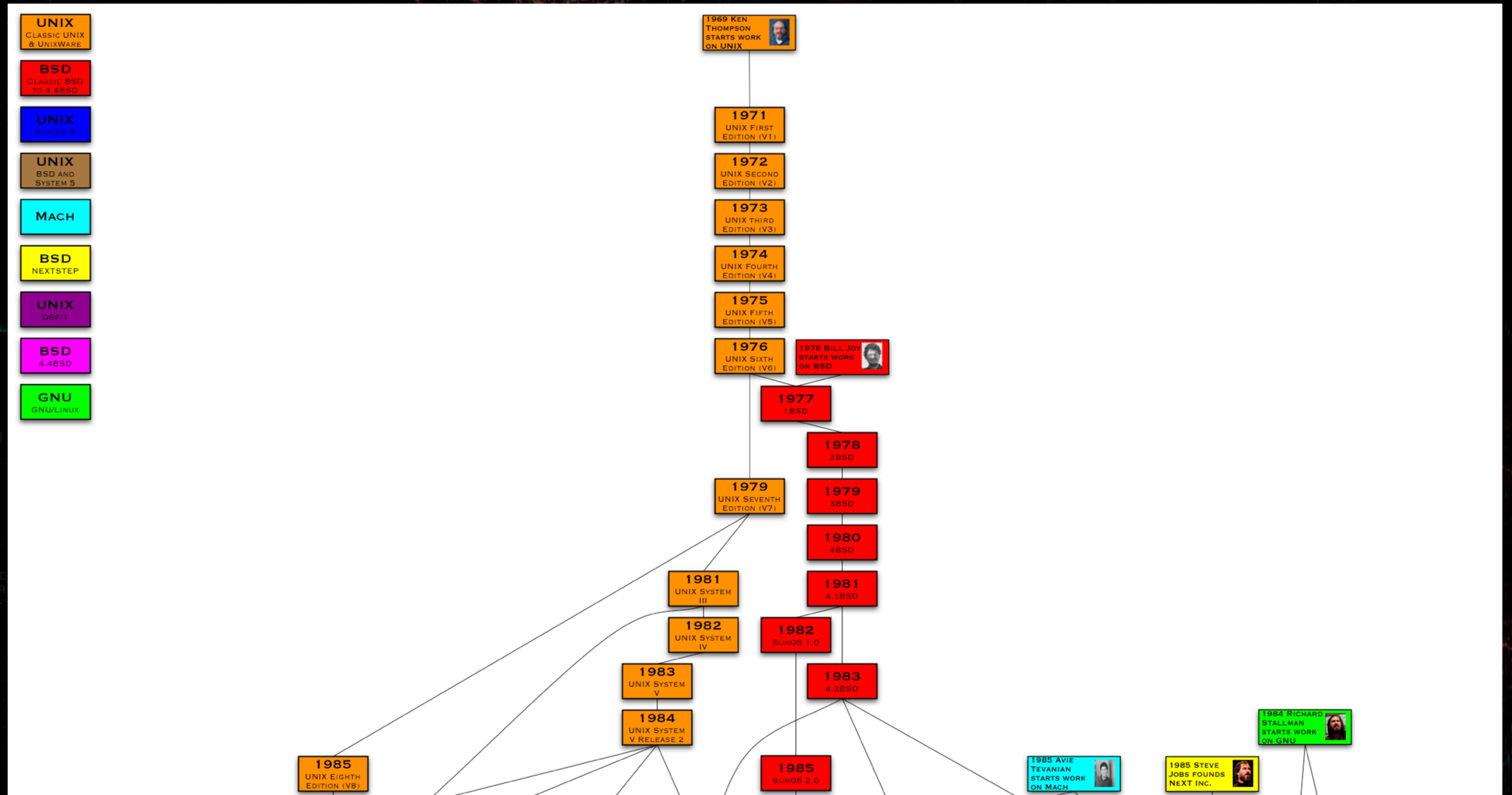
- Système d’exploitation en 1964 par les laboratoires Bell (filiale d’AT&T)



Le GE-645

Linux : monde libre, internet




UNIX
Classic UNIX & UnixWare
BSD
Classic BSD to 4.4BSD
UNIX
System 5
UNIX
BSD and System 5
Mach
BSD
NeXTSTEP
UNIX
OSF/1
BSD
4.4BSD
GNU
GNU/Linux
1969 Ken Thompson starts work on UNIX
1971
UNIX First Edition (V1)
1972
UNIX Second Edition (V2)
1973
UNIX Third Edition (V3)
1974
UNIX Fourth Edition (V4)
1975
UNIX Fifth Edition (V5)
1976
UNIX Sixth Edition (V6)
1976 Bill Joy starts work on BSD
1977
1BSD
1978
2BSD
1979
UNIX Seventh Edition (V7)
1979
3BSD
1980
4BSD
1981
UNIX System III
1981
4.1BSD
1982
UNIX System IV
1982
SunOS 1.0
1983
UNIX System V
1983
4.2BSD
1984
UNIX System V Release 2
1984 Richard Stallman starts work on GNU
1985
UNIX Eighth Edition (V8)
1985
SunOS 2.0
1985 Avie Tevanian starts work on Mach
1985 Steve Jobs founds NeXT Inc.

Quels sont les 5 systèmes d’exploitation les plus utilisés en 2023 sur ordinateur en France ?

- **Windows : 75,62 %**
- OS X : 17,9 %
- Système d’exploitation inconnu : 2,83 %
- Linux : 2,72 %
- Chrome OS : 0,86 %
- FreeBSD : 0,02 %

UNIX



Parts de marché des systèmes d’exploitation sur desktop en France en 2023

OS Mobiles

- Android : basé sur Unix



- iOS : basé sur Unix



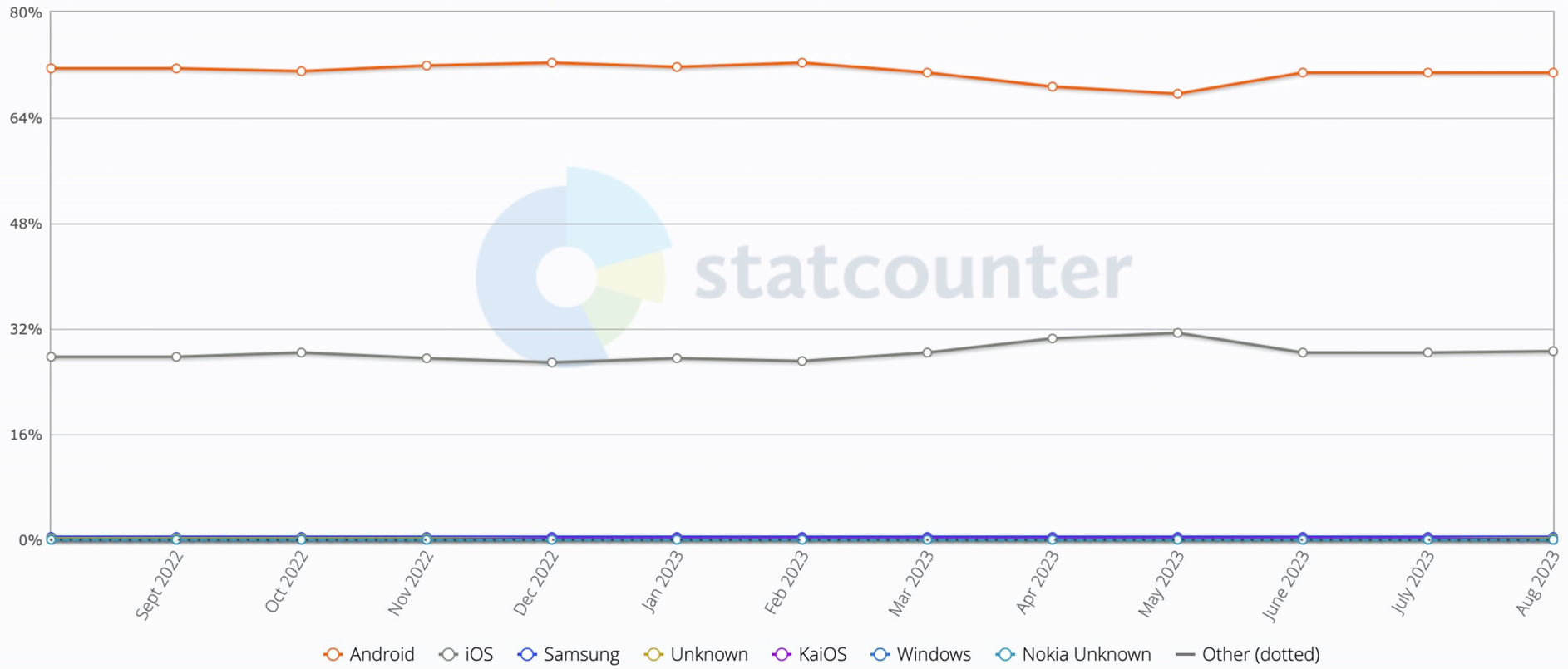
Android	iOS	Samsung	Unknown	KaiOS	Windows
70.77%	28.52%	0.37%	0.17%	0.1%	0.02%

Mobile Operating System Market Share Worldwide - August 2023

Mobile Operating System Market Share Worldwide

Aug 2022 - Aug 2023

Edit Chart Data



Serveurs



- 2/3 des serveurs web utilisent Linux
- 99,88% !!! des supercalculateurs utilisent Linux

Puissance des ordinateurs



En 2011, l'iPad 2 est aussi puissant qu'un supercalculateur de 1985

Standardisation

- SVID
  - System V Interface Definition – AT&T (1984)
  - A servi de base aux travaux du groupe POSIX
- POSIX
  - Portable Operating System Interface – IEEE (1986)
  - Standard définissant l’interface entre le système d’exploitation et les programmes d’application
  - Garantie la compatibilité source entre machines
  - Travaux non limité à Unix

Utilisateurs et Groupes

- Un utilisateur est caractérisé par :
  - Son login (nom de connexion)
  - Son appartenance à un groupe
- Contrôle de l'accès à la machine
  - Augmente la sécurité du système
  - Augmente la protection des utilisateurs
- Chaque utilisateur
  - est propriétaire des données qu'il crée
  - Définit les droits d'accès à ses données

Super utilisateur

- Un utilisateur ne peut effectuer des tâches d'administration du système pour des raisons de sécurité.
  - Exemple : arrêt de la machine, ajout d'un périphérique, création d'un utilisateur,…
- Le super utilisateur (root) est le seul à pouvoir effectuer:
  - N'importe quelle commande
  - Sur n'importe quelles données
- L'utilisateur « root » sert à gérer le système :
  - Créer ou radier des utilisateurs
  - Connecter des périphériques
  - Organiser l'espace disque
  - Optimiser la fonctionnement du système,…

Connexion

- L’écran affiche :
  - Login :
- L’ordinateur attend :
  - Un nom d’utilisateur et
  - Un mot de passe
- Ce qui entraîne :
  - La connexion au système
  - Un message d’invite (prompt)
  - L’attente d’une instruction
- Le mot de passe :
  - Protège l’accès au données de l’utilisateur
  - Doit rester confidentiel
  - Peut se modifier par la commande : **passwd**
  - Ne s’affiche jamais

Déconnexion

- Lorsqu'une session de travail est terminée, il faut se déconnecter du système.
- Trois commandes sont possibles :
  - logout
  - exit
  - Ctrl-D (^D) combinaison de la touche CTRL et D
- Les trois commandes sont équivalentes
- On peut aussi éteindre le système s'il est personnel.

Installation de LINUX


Training
Database
Kali Linux
Installation
Kali est basé
sur Debian

Kali Linux

- Kali Linux est une distribution de sécurité Linux dérivée de Debian et spécialement conçue pour l'investigation informatique et les tests d'intrusion avancés.

- Kali Linux contient plusieurs centaines d'outils bien conçus pour diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche en matière de sécurité, l'investigation informatique et l'ingénierie inverse.

- Les administrateurs de sécurité et les pirates Black Hat utilisent tous deux largement ce système d'exploitation. L’un pour détecter et prévenir les failles de sécurité, et l’autre pour identifier et éventuellement exploiter les failles de sécurité.



VMware Workstation Player







BTS CIEL — OPTION IR

Machines virtuelles

Faire tourner Linux dans Windows, sans toucher au disque

Qu'est-ce qu'une machine virtuelle ?

Un ordinateur complet simulé par logiciel : CPU, RAM, disque et carte réseau virtuels. L'OS installé dedans ne sait pas qu'il est virtuel.

HYPERVISEUR

La couche qui distribue les ressources physiques aux VM

HÔTE / HOST

La machine réelle et son système, ici Windows

INVITÉ / GUEST

Le système virtualisé, ici une distribution Linux

Architecture en couches

Linux invité — Ubuntu, Debian…

Autre VM — Windows Server, pfSense…

Matériel virtuel — vCPU, vRAM, disque .vdi/.vmdk, carte réseau virtuelle

Hyperviseur — VirtualBox, VMware Workstation, Hyper-V

Windows (système hôte)

Matériel physique — CPU avec VT-x / AMD-V, RAM, SSD

La virtualisation matérielle (VT-x / AMD-V) doit être activée dans le BIOS/UEFI.

VM ou dual-boot ?

CRITÈRE	MACHINE VIRTUELLE	DUAL-BOOT
Accès aux deux OS	Simultané, dans une fenêtre	Un seul à la fois, redémarrage
Disque	Un fichier, aucune partition	Repartitionnement du disque
Risque pour l'hôte	Isolé, erreur sans conséquence	Bootloader et données exposés
Retour arrière	Snapshot, clone, suppression	Réinstallation
Performances	Ressources partagées	Matériel dédié, natif

Cas d'usage en informatique et réseaux

01 — DÉVELOPPEMENT

Travailler dans l'environnement réel de production : shell, paquets, services systemd.

02 — RÉSEAU

Monter une maquette client / serveur / routeur sur un seul poste.

03 — SÉCURITÉ

Analyser un binaire suspect dans un bac à sable coupé du réseau.

04 — APPRENTISSAGE

Casser, restaurer un snapshot, recommencer en trente secondes.

Mise en place

HYPERVISEURS COURANTS

VirtualBox — gratuit, type 2, standard en formation

VMware Workstation Player — type 2, très stable

Hyper-V — type 1, inclus dans Windows Pro

EN CINQ ÉTAPES

1. Activer VT-x / AMD-V dans le BIOS
2. Installer l'hyperviseur
3. Télécharger l'image ISO de la distribution
4. Créer la VM : 2 vCPU, 4 Go de RAM, 30 Go de disque
5. Installer les additions invité, puis snapshot

Limites et coûts

8 Go

de RAM minimum sur l'hôte pour une VM confortable

~5 %

de perte CPU typique, mais les entrées/sorties disque souffrent davantage

GPU

accélération 3D limitée : pas de jeu ni de calcul CUDA sans passthrough

Pour un besoin purement ligne de commande, WSL 2 est plus léger. La VM reste nécessaire dès qu'il faut un noyau complet, un bureau graphique ou plusieurs machines en réseau.

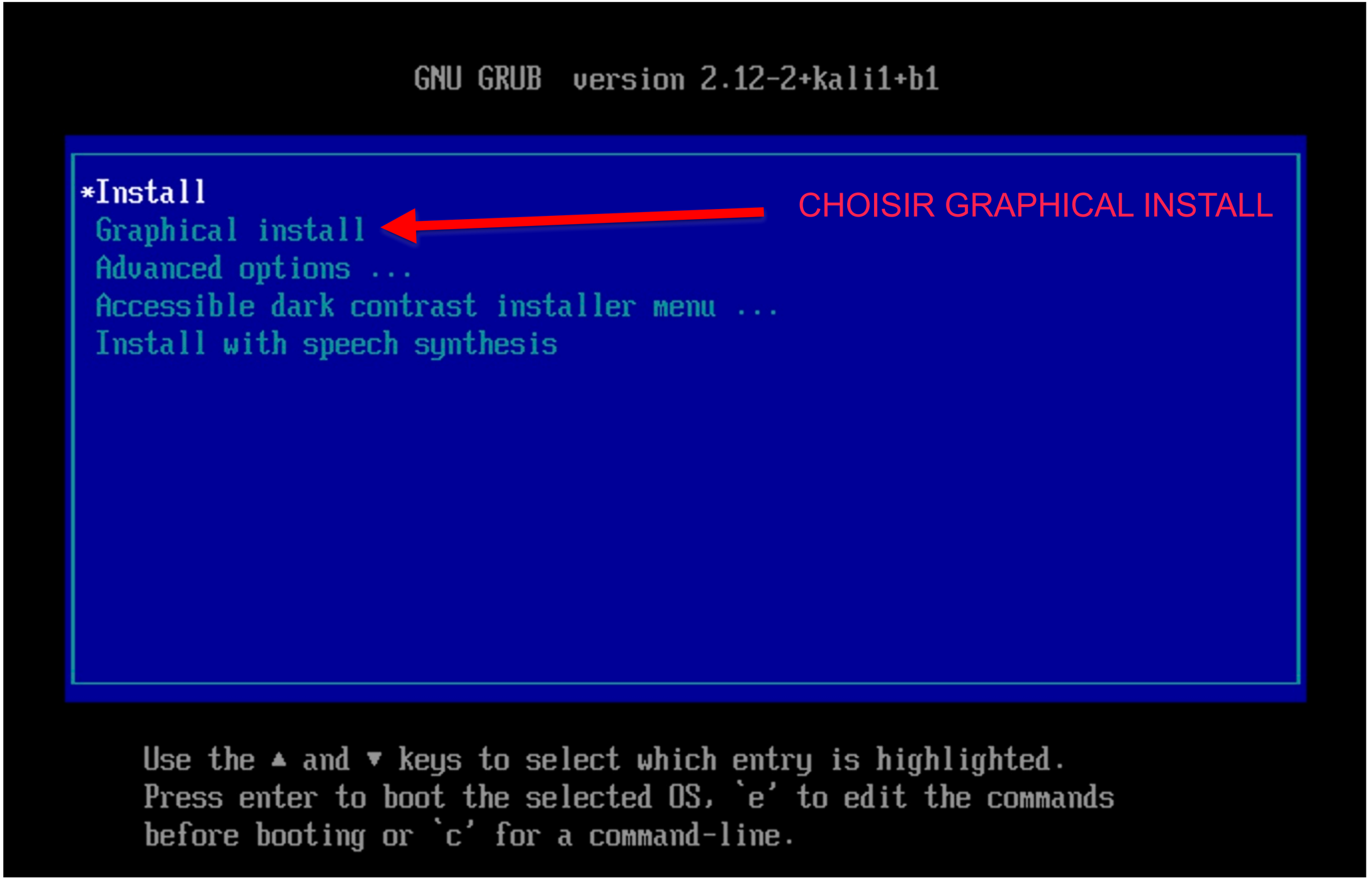
À RETENIR

Une VM apporte Linux dans Windows sans repartitionner, sans redémarrer et sans risque pour le poste.

Le prix à payer est un partage des ressources et un graphique limité. Pour apprendre, tester et maquetter, c'est le meilleur compromis.

- Installer une machine virtuelle (VirtualBox ou VMPlayer)
- Installer une image ISO de Kali Linux
- Taille disque VirtualBox : 30Go

Télécharger ou installer l’ISO fourni


GNU GRUB version 2.12-2+kali1+b1
*Install
Graphical install
Advanced options ...
Accessible dark contrast installer menu ...
Install with speech synthesis
CHOISIR GRAPHICAL INSTALL
Use the ▲ and ▼ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.


GNU GRUB version 2.12-2+kali1+b1
Install
*Graphical install
Advanced options ...
Accessible dark contrast installer menu ...
Install with speech synthesis
Use the ▲ and ▼ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.



Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Bulgarian	**-**	**Български**
Burmese	**-**	မြန်မာစာ
Catalan	**-**	**Català**
Chinese (Simplified)	**-**	中文(简体)
Chinese (Traditional)	**-**	中文(繁體)
Croatian	**-**	**Hrvatski**
Czech	**-**	**Čeština**
Danish	**-**	**Dansk**
Dutch	**-**	**Nederlands**
Dzongkha	**-**	རྫོང་ཁ
English	**-**	**English**
Esperanto	**-**	**Esperanto**
Estonian	**-**	**Eesti**
Finnish	**-**	**Suomi**
French	**-**	**Français**
Galician	**-**	**Galego**
Georgian	**-**	**ქართული**
German	**-**	**Deutsch**
Greek	**-**	**Ελληνικά**
Gujarati	**-**	ગુજરાતી
Hebrew	**-**	**עברית**
Hindi	**-**	हिन्दी

KALI

Choix de votre situation géographique

Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.

La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.

Pays (territoire ou région) :

- **Belgique**
- **Canada**
- **France**
- **Luxembourg**
- **Suisse**
- **Autre**

KALI

Configurer le clavier

Disposition de clavier à utiliser :

- Chinois
- Croate
- Tchèque
- Danois
- Néerlandais
- Dvorak
- Dzongkha
- Espéranto
- Estonien
- Éthiopien
- Finnois
- **Français**
- Géorgien
- Allemand
- Grec
- Gujarati
- Gourmoukhî
- Hébreu
- Hindi
- Hongrois
- Islandais
- Irlandais
- Italien

Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

kali

Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

btsciel

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

prof

Créer les utilisateurs et choisir les mots de passe

Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :

prof

Créer les utilisateurs et choisir les mots de passe

Make sure to select a strong password that cannot be guessed.

Choose a password for the new user:

●●●●●●

☐ **Afficher le mot de passe en clair**

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

●●●●●●

☐ **Afficher le mot de passe en clair**

Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

Assisté - utiliser un disque entier

Assisté - utiliser tout un disque avec LVM

Assisté - utiliser tout un disque avec LVM chiffré

Manuel

Partitionner les disques

Veuillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI1 (0,0,0) (sda) - 68.7 GB ATA Kali Linux 2024-

Partitionner les disques

Disque partitionné :

SCSI1 (0,0,0) (sda) - ATA Kali Linux 2024-: 68.7 GB

Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.

Schéma de partitionnement :

Tout dans une seule partition (recommandé pour les débutants)

Partition /home séparée

Partitions /home, /var et /tmp séparées

Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté

Configurer le RAID avec gestion logicielle

Configurer le gestionnaire de volumes logiques (LVM)

Configurer les volumes chiffrés

Configurer les volumes iSCSI

▽ SCSI1 (0,0,0) (sda) - 68.7 GB ATA Kali Linux 2024-

>		1.0 MB			Espace libre	
>	n° 1	536.9 MB	B	f	ESP	
>	n° 2	67.2 GB		f	ext4	/
>	n° 3	1.0 GB		f	swap	swap
>		1.0 MB			Espace libre	

Annuler les modifications des partitions

Terminer le partitionnement et appliquer les changements

Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
SCSI1 (0,0,0) (sda)

Les partitions suivantes seront formatées :
partition n° 1 sur SCSI1 (0,0,0) (sda) de type ESP
partition n° 2 sur SCSI1 (0,0,0) (sda) de type ext4
partition n° 3 sur SCSI1 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

○ **Non**

◉ **Oui**

Sélection des logiciels

Actuellement, seul le système de base est installé. Les pré-sélections ci-dessous installeront Kali Linux avec son environnement de bureau et ses applications par défaut.

Vous pouvez personnaliser votre système en choisissant un autre environnement de bureau et/ou une autre collection d'outils.

Logiciels à installer :

- [x] **Environnement de bureau [sélectionner cet élément n'a aucun effet]**
- [x] **... Xfce (environnement de bureau par défaut de Kali)**
- [ ] **... GNOME**
- [ ] **... KDE Plasma**
- [x] **Collection d'outils [sélectionner cet élément n'a aucun effet]**
- [x] **... top10 -- les 10 outils les plus populaires**
- [x] **... par défaut -- outils recommandés (disponibles dans le système live)**

Choisir et installer des logiciels



Préparation de haveged (arm64)

Utilitaire de démarrage

Installer « GRUB » à la fin

Par défaut c'est le « non » qui est sélectionné, choisissez « oui » pour Grub

Configuration Kali Linux

Clavier, écran, update

Clavier français

- S'il s'agit de l' environnement graphique, saisir dans un terminal la commande suivante:

  setxkbmap fr

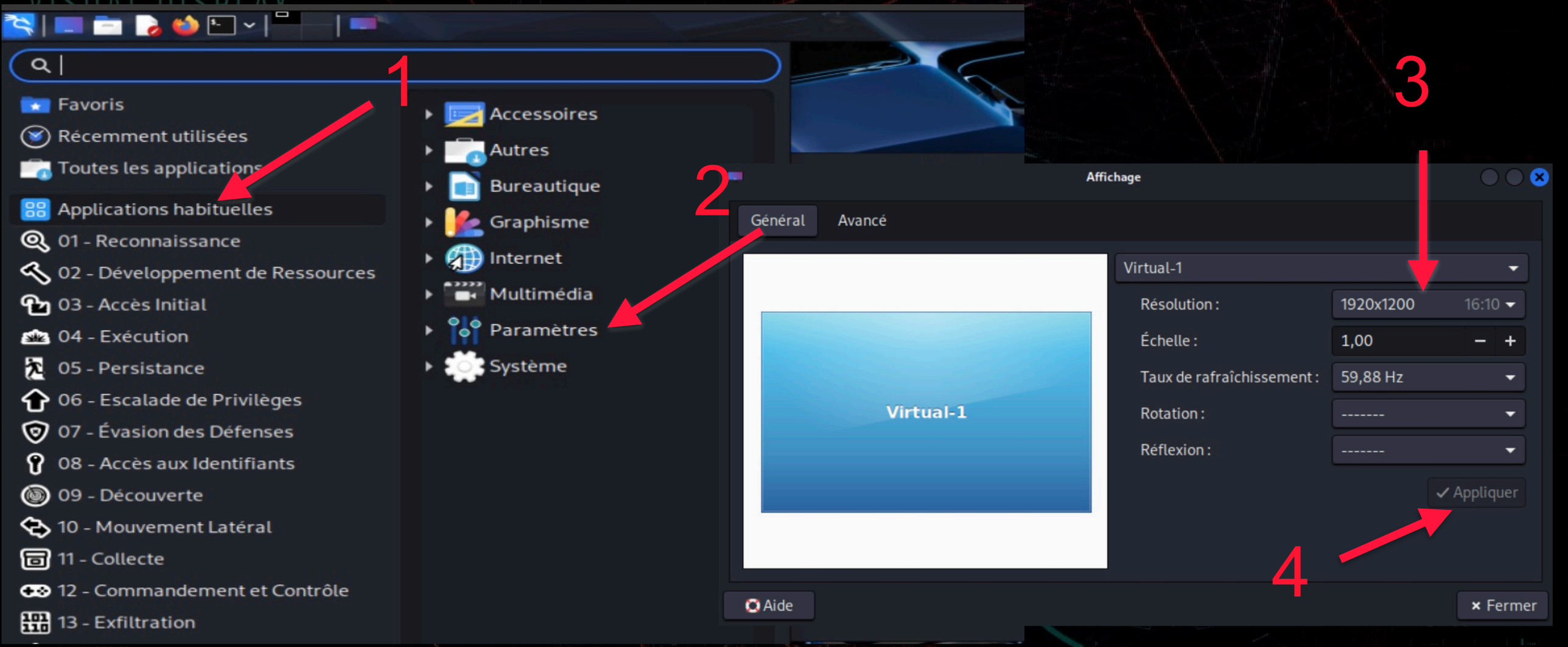
- Se traduira par la frappe de :

- setxkb**,q**p fr , si votre clavier est marqué AZERTY,

- Pour que votre Linux soit entièrement configurée avec votre nouveau clavier, y compris sur l'écran de login et la console de secours, saisissez dans un terminal la commande suivante:

  sudo dpkg-reconfigure keyboard-configuration

- Une interface semi-graphique vous offrira alors la possibilité de modifier comme vous l'entendez chacun des paramètres liés à votre clavier.
- Après validation de tous vos choix et un retour au prompt dans votre console, redémarrez votre machine pour que les modifications soient effectives. Les changements sont immédiats dans une console tty.


1
2
3
4
Favoris
Récemment utilisées
Toutes les applications
Applications habituelles
01 - Reconnaissance
02 - Développement de Ressources
03 - Accès Initial
04 - Exécution
05 - Persistance
06 - Escalade de Privilèges
07 - Évasion des Défenses
08 - Accès aux Identifiants
09 - Découverte
10 - Mouvement Latéral
11 - Collecte
12 - Commandement et Contrôle
13 - Exfiltration
Accessoires
Autres
Bureautique
Graphisme
Internet
Multimédia
Paramètres
Système
Affichage
Général
Avancé
Virtual-1
Résolution :
1920x1200
16:10
Échelle :
1,00
Taux de rafraîchissement :
59,88 Hz
Rotation :
Réflexion :
Appliquer
Aide
Fermer

Compte sudo

- la commande "sudo" permet de se donner les droits "root"

- Si Debian dit que le compte n'apparaît pas dans le fichier sudoers, il faudra alors l'ajouter, pour cela :

- Passer en mode "root" en tapant "su", entrer le mot de passe

  - editer le fichier avec : gedit /etc/sudoers

  - Copier la ligne avec "root" et changer root par le nom de votre utilisateur :
    root ALL=(ALL:ALL) ALL
  - Par exemple :
    root ALL=(ALL:ALL) ALL
    prof ALL=(ALL:ALL) ALL
    Sortir du mode "root" en tapant exit

Syntaxe des commandes Unix

- Forme générale des commandes :

```
Commande –abc… arg1 arg2 …
```

  - Nom de commande
  - Options
  - Arguments : données à traiter

- Les majuscules et les minuscules sont différentes :

  Exemple :
  Date ≠ date

- Les commandes Unix sont entrées en minuscules (sauf certaines options)
- Dans la suite

  $> message d'invite d'instructions

Le terminal

- Ouverture d’une fenêtre de terminal pour entrer les commandes Shell
- Créer un raccourci pour retrouver plus facilement le terminal

Exemples de commandes

- Afficher la date et l’heure :
  $> date
- Afficher le calendrier :
  $> cal
- Qui est connecté ?
  $> who
- Sous quel login suis-je connecté ?
  $> whoami
- Liste des fichiers
  $> ls
- Nom de l’OS
  $> uname
- Version de l’OS
  $> uname -r
- Nom de l’OS
  $> uname
- Nom de la machine
  $> hostname

Les fichiers

- Le fichier représente une unité de stockage des données en mémoire de masse (support « permanent »)
- Un fichier est identifié par un nom et une localisation en mémoire de masse
- Les noms sont une chaîne de caractères composé de :
  Lettres, chiffres et caractères spéciaux (. _ - …)
- Ils se présentent souvent sous la forme :
  Prefixe.suffixe
- Les majuscules et les minuscules sont différentes

Commandes sur les fichiers

- ls : affiche la liste des fichiers
- Options
  - ls –l : liste détaillée
  - ls –a : donne en plus les fichiers cachés (le nom commence par un point) et tous les sous-répertoires
  - ls –t : affiche la liste par ordre anté-chronologique
- Il est possible de combiner plusieurs de ces options :
  - Exemples : ls –la, ls –lt

Aide sur les commandes

- sur internet :
  - rechercher « nom commande » + linux
- en ligne de commande :
  - « $ man commande »
- historique des commandes :
  - « $ history »

Joker

- Permet de remplacer un ou plusieurs caractères dans un nom de fichier
- Le joker * remplace n’importe quel chaîne de caractères (même vide)
- Le joker ? remplace n’importe quel caractère
- Exemples :
  - ls a*
  - ls *.d??

Les répertoires

- Ils permettent d’organiser et de classer les fichiers
- Un répertoire (directory) contient :
  - Des fichiers,
  - Des sous-répertoires, pouvant contenir d’autres fichiers et sous répertoires

  ➢Ce qui donne lieu à une arborescence
- La racine (root) est notée : /

Identification d’un fichier

- Un fichier est identifié par un chemin d’accès
- Le chemin d’accès absolu commence toujours par / (root, la racine)
  - /usr
  - /home/ESI/rep/
- La racine (root) est notée : /

Répertoire courant

- Est le répertoire dans lequel se trouve un utilisateur à un instant donné : symbolisé par un point (.)
- **pwd** (Print Working Directory) : affiche le répertoire courant
- **cd** (Change working Directory) : change de répertoire courant :
  - Lorsque cette commande est introduite sans argument, le nouveau répertoire courant devient le répertoire de connexion : répertoire par défaut lorsque l'utilisateur se connecte.
- **cd ..** : remonte dans l'arborescence

Protection des fichiers

- Objectifs :
  - Sécurité du système
  - Confidentialité des données
- Trois niveaux de protection :
  - Le propriétaire : owner
  - Le groupe d’utilisateur : group
  - Les autres utilisateurs : others
- Trois types de protections
  - r : lecture : Read
  - w : écriture : Write
  - x : execution : eXecute

Exemple de protection

```
-rwxr-xr--  1 dupont francais 125 Janv 7 10:15 fichier.txt
```



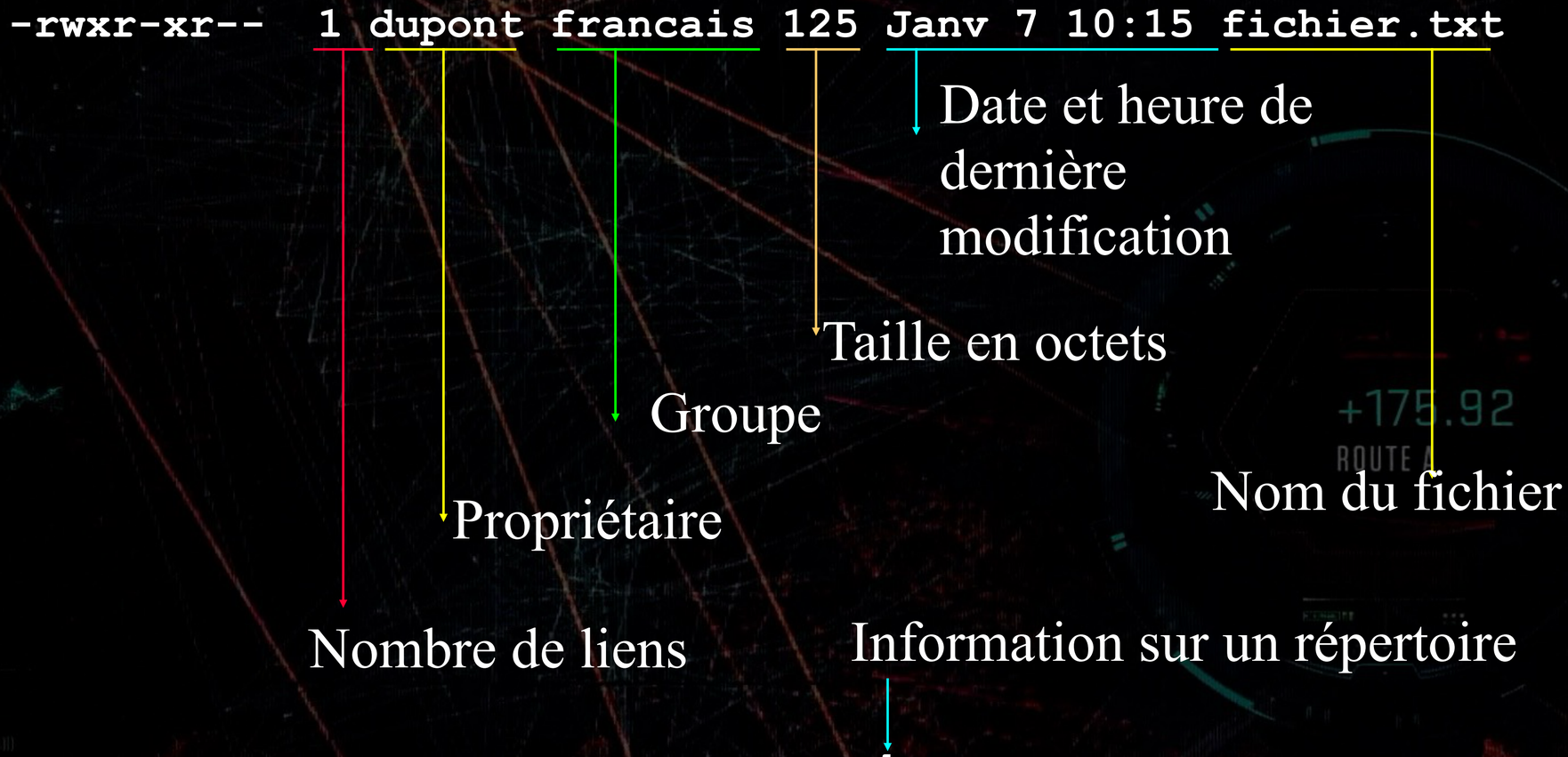
Accessible uniquement en lecture aux autres

Accessible en lecture et exécution au groupe «francais»

Accessible en lecture, écriture et exécution au Propriétaire « dupont »

Fichier simple (ce n’est pas un répertoire)

Informations sur un fichier



Droits en octal

- Les droits peuvent également être représentés en octal
- Octal = base 8 : de 0 à 7 , de 000 à 111
- Exemple : r w x - - x - - x
- 1 1 1 0 0 1 0 0 1
- 7 1 1

Edition d’un texte

- nano nom_du_fichier

- Observez les attributs du fichier grâce à la commande "ls –l"

Changement des protections

- **chmod** modifie les droits d'accès d'un fichier ou d'un répertoire
- Syntaxe :
  - chmod [*qui*]*permissionopération nom_fichier*
  - *qui* une combinaison de lettres
    - u pour le propriétaire (user)
    - g pour le groupe (group)
    - o pour les autres utilisateurs (others)
    - a pour tous (all), valeur par défaut
  - *permission* est
    - + pour autoriser
    - - pour interdire
    - = pour donner certaines permissions et supprimer les autres
  - *opération* est une combinaison de lettres
    - r : lecture : Read w : écriture : Write x : execution : eXecute

Exercice

- Ajouter des droits de modification au groupe :
  - chmod g+w fichier
  - ls -l
- Les retirer :
  - chmod g-w fichier
  - ls -l
- En octal : tous les droits u, aucun pour les autres
  - chmod 700 fichier

Visualisation

- Pour visualiser le contenu d’un fichier il y a au moins deux commandes :
  - Pour les petits fichiers, la commande cat
  - Pour les fichiers plus grand, la commande more nom-du-fichier fera un affichage par page en ligne de commande, barre d’espace pour la page suivante, touche ‘B’ pour revenir en arrière (Back)
- more /etc/os-release

Commandes sur les répertoires
Création

- **mkdir** : création d'un répertoire
  - Elle est conditionnée au droit de l'utilisateur
- Syntaxe :
  - mkdir *nom_de _répertoire*
- Le nom de répertoire à créer peut être indiqué
  - En absolu : mkdir /home/user/rep/
  - En relatif : mkdir rep

Destruction d’un répertoire

- **rmdir** : détruit un répertoire
  – Elle est conditionnée au droit de l’utilisateur
- Syntaxe :
  – rmdir *nom_de _répertoire*
- Pour être détruit, un répertoire doit être vide
- **rm –r** : destruction d’un répertoire et des sous-répertoires

▲Attention il n’est pas possible de revenir en arrière ! (pas de corbeille !)

Destruction

- **rm** détruit un fichier ou un répertoire (ReMove)
- Syntaxe :
  - rm *nom_fichier*
- Options
  - -i demande une confirmation avant destruction
  - -r détruit le répertoire et les fichiers/répertoires qu'il contient
- ▲ Attention il n'est pas possible de revenir en arrière!

Copies

- **cp** duplique un fichier ou un répertoire
- ▲ Si le fichier destination existe déjà, il est écrasé !
- Options :
  - **cp -r** : duplique un répertoire sous un autre répertoire
  - **cp –i** : interroge avant la copie
- Syntaxe :
  - cp *origine destination*

Renommage

- **mv** renomme ou déplace un fichier ou un répertoire (MoVe)

▲ Si le fichier destination existe déjà, il est écrasé !

- Syntaxe :
  – Change le nom d'un fichier ou d'un répertoire :
  mv *nom_actuel nouveau_nom*
  – Déplace un fichier ou un répertoire
  mv *origine destination*

☞ mv sur un répertoire déplace toute la hiérarchie du répertoire

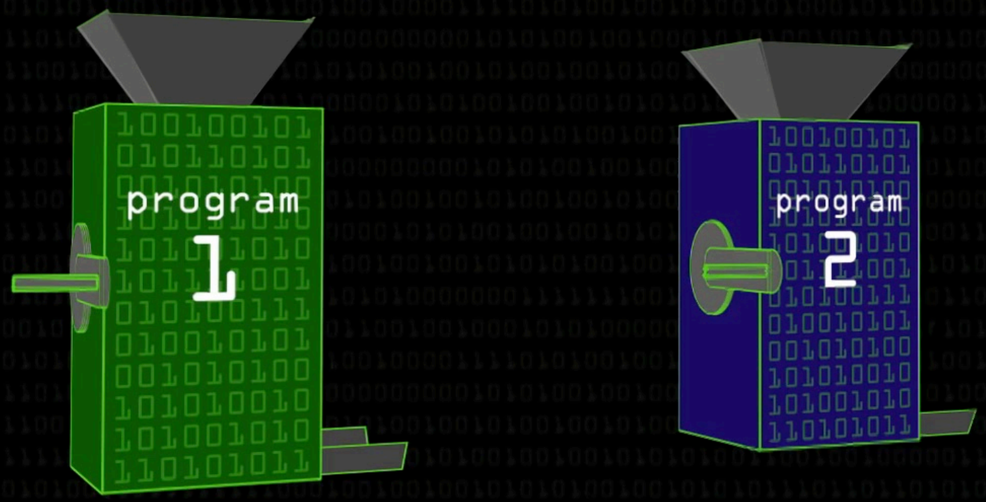
Exercices

- Créer un répertoire
- Visualiser les attributs (avec ls -l)
- Renommer ce répertoire (avec mv)
- Supprimer le
- Vérifier la suppression avec ls -l

Installation et utilisation d'applications LINUX

- Gestionnaire de fichiers
- Terminal administrateur
- Filezilla Client : client FTP
  - apt install filezilla
- Libre Office : équivalent Microsoft Office
  - apt install libreoffice
- Wireshark : capture et analyse de trames
- ...

Pipeline – Tube : |



Tube ou « pipe »

- On peut utiliser la sortie d’une commande pour l’envoyer sur une autre et ainsi combiner plusieurs commandes entre elles.
- Par exemple, lorsque l’on fait la liste des fichiers, on peut l’envoyer sur l’affichage page par page.
- Exemple :
  - cd /etc
  - ls –l | more

Redirection

- On peut aussi rediriger une sortie écran vers un fichier grâce à « > » et « >> »
- Exemple : ls –l > liste.txt
- « > » créé un nouveau fichier et écrase l’ancien s’il existait déjà, « >> » ajoute les données au fichier existant
- Vérifier l’existence du fichier par ls -l
- Afficher le contenu par : more liste.txt
- cd (revenir dans votre répertoire)
- ls -l /etc > liste.txt

Commande GREP

- Recherche une chaine de caractères dans un ou plusieurs fichiers textes et affiche à l'écran les lignes contenant cette chaine
- Syntaxe :
- grep [Options] modèle [Fichier1...]
- options intéressantes :

  -v effectue la recherche inverse : toutes les lignes ne correspondant pas aux critères sont affichées.

  -c ne retourne que le nombre de lignes trouvées sans les afficher.

  -i ne différencie pas les majuscules et les minuscules.

  -n indique le numéro de ligne pour chaque ligne trouvée.

  -l dans le cas de fichiers multiples, indique dans quel fichier la ligne a été trouvée.

```
$ cat depts.txt
73      82      82121   0       TARN-ET-GARONNE Tarn-et-
Garonne
93      83      83137   2       VAR     Var
93      84      84007   0       VAUCLUSE        Vaucluse
52      85      85191   3       VENDEE  Vendée
54      86      86194   3       VIENNE  Vienne
74      87      87085   3       HAUTE-VIENNE    Haute-Vienne
41      88      88160   4       VOSGES  Vosges
26      89      89024   5       YONNE   Yonne
$ grep 85191 depts.txt
52      85      85191   3       VENDEE  Vendée
```

Utilisation d'une expression régulière insensible à la casse

```
$ grep -E -i '(paris|vosges)' depts.txt
11      75      75056   0       PARIS   Paris
41      88      88160   4       VOSGES  Vosges
```

Afficher les lignes ne commençant pas par le chiffre 9

```
$ grep -v '^9' depts.txt
73      82      82121   0       TARN-ET-GARONNE Tarn-et-Garonne
52      85      85191   3       VENDEE  Vendée
54      86      86194   3       VIENNE  Vienne
74      87      87085   3       HAUTE-VIENNE    Haute-Vienne
41      88      88160   4       VOSGES  Vosges
26      89      89024   5       YONNE   Yonne
```

Automatisation CRON

- Le service cron permet la programmation d’événements à répétition.
- Il fonctionne à l’aide d’une table, appelée une crontab.
- C’est un fichier texte, éditable avec un simple éditeur.
- Pour modifier votre crontab personnelle utilisez la commande crontab pour éditer la table, avec le paramètre -e, pour lister les tâches en cours -l

Automatisation CRON

- Le service cron doit tourner pour que les crontabs soient actives.
- Commande terminal : ps -ef | grep cron
-

```
prof@prof-Ubuntu:~$ ps -ef|grep cron
root         603       1  0 09:57 ?        00:00:00 /usr/sbin/cron -f
prof        4500    1612  0 10:02 pts/0    00:00:00 grep --color=auto cron
```

Minutes	Heures	Jour du mois	Mois	Jour semaine	Commande
1	2	3	4	5	6

- Format d’un enregistrement de crontab
- Utilisez le format suivant pour les valeurs périodiques :
  - Une valeur pour indiquer quand il faut exécuter la commande. Ex : la valeur 15 dans le champ minute signifie la quinzième minute.
  - Une liste de valeurs séparées par des virgules. Ex : 1,4,7,10 dans le champ mois pour janvier, avril, juillet, octobre.
  - Un intervalle de valeurs. Ex : 1-5 dans le champ jour de la semaine indique du lundi (1) au vendredi (5). Le 0 est le dimanche et le 6 le samedi.
  - Le caractère * pour toutes les valeurs possibles. Ex : * dans le champ jour du mois indique tous les jours du ou des mois.

Exemples CRON

Minutes	Heures	Jour du mois	Mois	Jour semaine	Commande
1	2	3	4	5	6

- Exécution de df tous les jours, toute l'année, tous les quarts d'heure :
- `0,15,30,45 * * * * save_bdd`
- Exécution d'une commande tous les jours ouvrables à 17 heures :
- `0 17 * * 1-5 fin_travail.sh`
- Lister les crontabs actives :
  $ crontab -l

Exercices CRON

Minutes	Heures	Jour du mois	Mois	Jour semaine	Commande
1	2	3	4	5	6

- Quel est l'effet de la ligne crontab suivante * * * * * who > /tmp/test ?
- Quelle ligne crontab écrire pour lancer la commande checkall du lundi au vendredi à 23h, seulement au mois de juin ?
  - A - * 23 * 6 1,5 checkall
  - B - 0 23 0 6 1-5 checkall
  - C - 23 * 6 1-5 checkall
  - D - 0 23 * 6 1-5 checkall

Correction exercices CRON

Exercices CRON

- Quelle commande permet d’éditer la crontab ?
- Quelle commande permet de lister les tâches crontab ?
- Vous devez lancer une tâche appelée script.sh tous les soirs à 21h00. Quelle est la commande à taper ?

Correction exercices CRON

Travaux pratiques CRONTAB

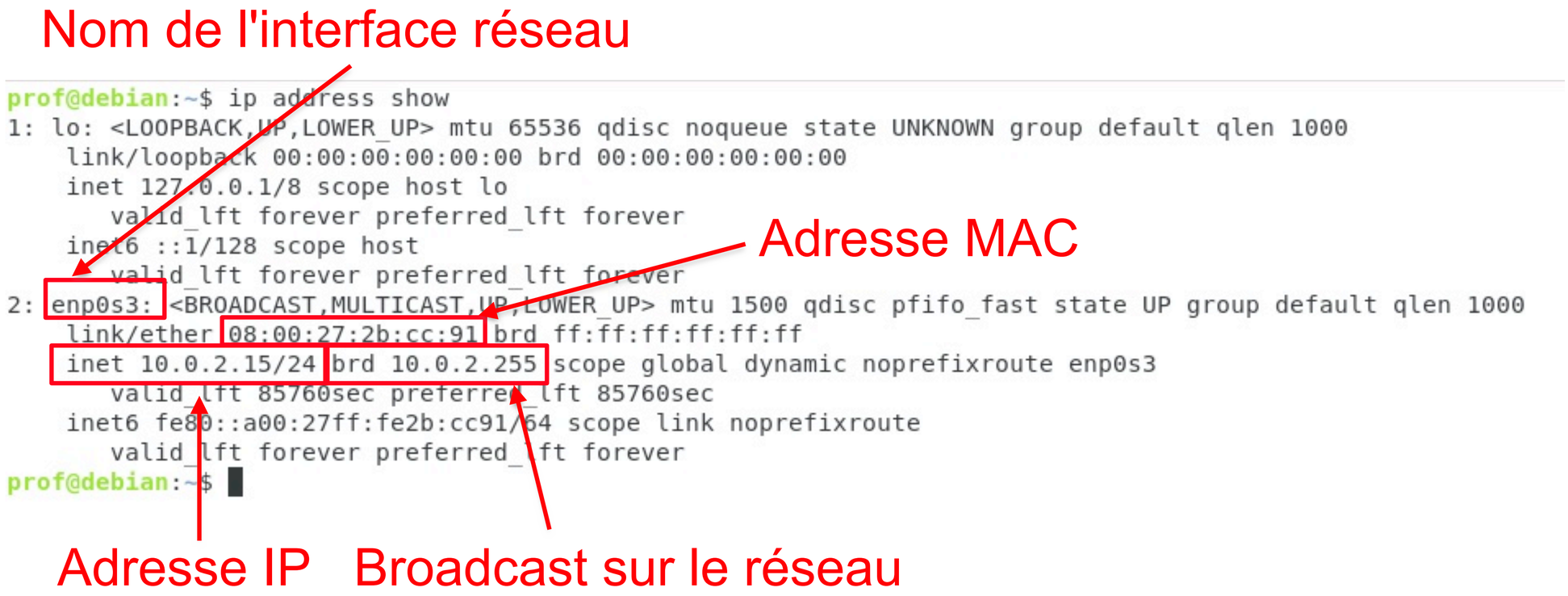
- Ouvrir une fenêtre de terminal
- Lancer la commande : crontab -l
- Créer une tâche planifiée avec crontab -e
- Choisir l'éditeur
- On veut écrire la date toutes les minutes dans un fichier texte

- Modifier la tâche pour ajouter la date aux précédentes.
- Ajouter le texte « Bonjour » toutes les minutes dans le fichier

- Quitter (^X CTRL X) en sauvegardant, lister les tâches, vérifier le contenu du fichier date.txt
- Supprimer la tâche que vous venez de créer.

Voir l'adresse IP

- Commande : ip address show
- ou : ip addr ou : ip a
- Sur d'anciens systèmes : ifconfig



NMAP

Outil d'exploration réseau et scanneur de ports/sécurité

Nmap (« Network Mapper ») est un outil open source d'exploration réseau et d'audit de sécurité. Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique

Nmap innove en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés

MAN NMAP

POUR AVOIR TOUTES LES OPTIONS

ET EXPLICATIONS

Si non installé,
apt install nmap
en root

Config réseau machine virtuelle

- Pour voir les autres machines, il faut être dans le même réseau
- Se connecter au réseau du BTS CIEL
- Dans la configuration réseau de la machine virtuelle, choisir « Accès par pont » ou « Bridge »
- Redémarrer Linux
- Lire l’adresse IP par « ip a », vérifier l’adresse réseau
- Faire la commande « nmap -sn 192.168.1.1/24 »

```
┌──(prof㉿kali)-[~]
└─$ nmap -sn 192.168.1.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 16:25 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
MAC Address: 00:0D:B4:28:7E:8D (Stormshield)
Nmap scan report for 192.168.1.2
Host is up (0.0014s latency).
MAC Address: 4C:CC:6A:48:F7:07 (Micro-Star Intl)
Nmap scan report for 192.168.1.21
Host is up (0.0017s latency).
MAC Address: 00:41:D2:A0:9C:A0 (Cisco Systems)
Nmap scan report for 192.168.1.22
Host is up (0.0017s latency).
MAC Address: 00:41:D2:A0:A3:60 (Cisco Systems)
Nmap scan report for 192.168.1.30
Host is up (0.0017s latency).
MAC Address: F0:2F:74:B2:F0:EC (ASUSTek Computer)
Nmap scan report for 192.168.1.32
Host is up (0.0017s latency).
MAC Address: 8C:DC:D4:40:83:8E (Hewlett Packard)
Nmap scan report for 192.168.1.34
Host is up (0.0017s latency).
MAC Address: 20:9B:E6:6D:66:A6 (Guangzhou Shiyuan Electronic Technology Company Limited)
Nmap scan report for 192.168.1.42
Host is up (0.13s latency).
MAC Address: 90:0F:0C:4B:03:1F (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.47
Host is up (0.00087s latency).
MAC Address: F0:2F:74:B2:F1:2B (ASUSTek Computer)
```

ROUTE

Permet de lister la table de routage de la machine Linux

```
prof@debian:/etc/network/interfaces.d$ route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
prof@debian:/etc/network/interfaces.d$
```

man route

pour avoir toutes les options

ip route

```
prof@debian:/etc$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
prof@debian:/etc$
```

TRACEROUTE

Permet de lister toutes les passerelles utilisées pour accéder à une adresse IP ou un serveur web

```
prof@debian:/etc/network/interfaces.d$ traceroute www.google.fr
traceroute to www.google.fr (172.217.22.131), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.178 ms  0.150 ms  0.130 ms
 2  m1login.net (192.168.10.1)  3.950 ms  3.928 ms  3.992 ms
 3  10.48.0.1 (10.48.0.1)  37.185 ms  37.177 ms  37.277 ms
 4  192.168.253.30 (192.168.253.30)  37.099 ms  43.466 ms  44.979 ms
 5  192.168.255.18 (192.168.255.18)  44.965 ms  45.020 ms  45.081 ms
 6  194.149.165.229 (194.149.165.229)  45.091 ms  32.468 ms  32.491 ms
 7  ppp86-metz.isdnet.net (194.149.166.213)  32.449 ms  31.663 ms  31.634 ms
 8  72.14.220.83 (72.14.220.83)  50.677 ms  50.778 ms  50.836 ms
 9  google.mix-it.net (217.29.66.96)  45.810 ms  47.960 ms  52.323 ms
10  108.170.245.89 (108.170.245.89)  52.280 ms 108.170.245.83 (108.170.245.83)
11  172.253.71.227 (172.253.71.227)  64.047 ms  64.168 ms  64.085 ms
12  216.239.35.207 (216.239.35.207)  63.947 ms 216.239.35.201 (216.239.35.201)
13  209.85.255.107 (209.85.255.107)  57.804 ms 108.170.238.163 (108.170.238.163)
14  108.170.245.1 (108.170.245.1)  61.800 ms  69.326 ms 108.170.244.193 (108.170
15  66.249.95.103 (66.249.95.103)  44.891 ms 66.249.95.247 (66.249.95.247)  46.0
16  par21s12-in-f3.1e100.net (172.217.22.131)  52.987 ms  62.171 ms  60.873 ms
prof@debian:/etc/network/interfaces.d$
```

INSTALLATIONS SUR KALI LINUX

- Ouvrir le terminal administrateur
- apt update
- apt install libreoffice
- apt install filezilla
- apt install wireshark