**Anneaux de protection**

Le processeur crée les anneaux de protections, pas le kernel.

* 0 : mode superviseur (kernel)
* 1
* 2
* 3 : user

En mode virtualisation, le 0 est l’hyperviseur et le 1 est le kernel.

**Périphériques**

* Mode caractère : flux d’octets
* Mode bloc : ex sda
* Network

1 numéro majeur (pilote)

1 numéro mineur (le périph)

Chaque périph possède un UUID.

**Kernel**

* Vmlinuz : image kernel
* System.map : symboles du noyau
* Initrd : chargement des drivers

Dépendance entre ces fichiers et régérés à chaque compil.

**Modules**

**Disks**

* LVM : logical volume manager
* Partition classique

Partition = partie du DD destiné à accueillir un système de fichier

Table des partitions :

Formattage – partitionnement – création swap/FS

**Directories**

**boot/** Bootloader, initrd, kernel…

**proc/** Pseudo fichier, occupe 0 octets en mémoire.

**XX/ :** PID processus en exec

**acpi/wakeup/** Liste des devices permettant de sortir de veille prolongée

**bus/**

**cmdline/ :** Params passés au noyau lors de son chargement

**cpuinfo/**

**crypto/ :** tous les algos installés et utilisables

**devices/ :** Tous les periph blocs et caractères du système.

**Filesystems/ :** Tous les VFS pris en compte.

**Interrupts/ :** Liste des IRQ par proc

**Iomem/ :** @RAM utilisés

**Ioports/ :**

**Irq/**

**Kcore/ :** Représente la RAM du système

**Loadavg/ :** Charge du système

**Meminfo/ :** Usage de la RAM

**Modules/ :** Modules chargés par le noyau

**Mounts/ :** Lien symbolique, table de montage

**Net/ :** Lien symbolique, accès aux tables ARP, routage, sockets…

**Partitions/ :**

**Swaps/ :** Infos sur le swap du système

**-uptime :** Temps écoulé en secondes depuis démarrage et durée d’inactivité

**-loadavg :** Charge moyenne depuis 1, 5, 15 min, #process, PID dernier process utilisé

**-version** : version du noyau (pae = physical adress extension = jusqu’à 64 Go de RAM).

**-vmallocinfo :** Infos sur la mémoire virtuelle

**sys/** Fichiers de conf du kernel

**kernel/ -pid-max :** Valeur du PID-max

**sys/** Pseudo fichier, occupe 0 octets en RAM

**etc/** Confs.

**passwd/ :** User infos

Username, passwd, UID, GID, UID infos, Home directory, Shell (or cmd)

**shells/ :** Shells valides.

**Shadow/ :** User passwd infos.

* Username
* Hash : $1$ MD5, $2a$ Blowfish, $5$ SHA 256, $6$ SHA 512

$X$ SALT $ HASH

* LastChanged : UNIX format (1970)
* Min : #days between Passwd changes.
* Max : #days valid
* Warn : #days before receiving warning.
* Inactive : #days after passwd expires : disabling.
* Expire : Absolute date which acount expires.

**-login.defs :** Conf for **new** users acount

**Skel/ :** Fichiers copiés dans le répertoire du user lors de sa création

**Group/ :** Name :mdp :GID :member1, member2…

**Gshadow/ :**

**pam.d/ :** Conf des services utilisant PAM

**fstab/ :** Liste des periph montés automatiquement au démarrage

**-Os-release**

**-services :** Ports -> Portname

**-hostname**

**-resolv.conf :** Serveurs DNS

**bin/**

**sbin/**

**lib/** .a = lib that contains many .o / .so = shared lib / lib linked to /bin /sbin

**usr/ bin/**

**sbin/**

**lib/** Linked to /usr/bin /usr/sbin

**dev/** Periph access

**mnt/** Point de montage temp

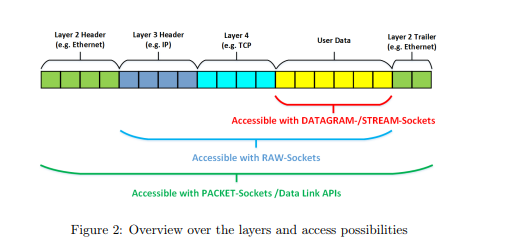
**opts/** Applications tierces (non issues de la distrib)

**tmp/**

**var/**

**Network**

Enp0s1 : ethernet bus 0 slot 1



Kernel doit être compilé pour accepter l’utilisation des sockets RAW.

UNIX\_SOCKET : mode utilisateur

RAW\_SOCKET : couche 3

PACKET\_SOCKET : couche 2

Librairies : Libpcap, libnet.

**Démarrage**

* BIOS effectue le POST (Power On Self Test : test des composants)
* BIOS charge le MBR : 512 premiers octets (table de partitions principale + bootloader = chargeur d’amorçage)
* GRUB
* Kernel se charge, init pilotes, démarre process kswapd et monte /
* Kernel démarre Init : PID 1 ne possède pas de père et père de tous les processus

Init = sysVinit, upstart ou systemd

* Démarrage des services (Debian 1-5 : sysVinit, Debian 6-7 : upstart, Debian >7 : systemd)

**Processus**

Espace mémoire process :

* 1 Go pour le noyau
* Instructions
* Biblios
* Pile (Var + @back)
* Tas ( malloc…)

PID jusqu’à 32768

Etats d’un process : Actif, exécutable, endormi, zombie.

**Authentification**

PAM : Pluggable authentication module

Entre l’utilisateur et le service demandé.

Conf des services utilisant PAM dans /etc/pam.d/