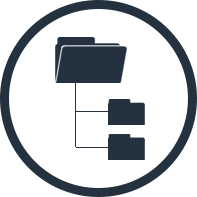
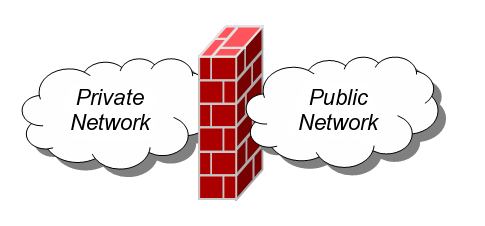
Secure Embedded System (SeS)

SSHD FileSystem Firewall

Auteur : Spinelli Isaia

Prof : [Schuler Jean-Roland](https://mse.hes-so.ch/consultation/master/horairesMSE.php?annee=2020&id=81&type=1)

Date : 26.10.2020

Salle : A4 – Lausanne

Classe : SeS

Table des matières

[Introduction - 2 -](#_Toc55232466)

[SSHD - 2 -](#_Toc55232467)

[Introduction - 2 -](#_Toc55232468)

[Installer et vérifier la signature d’OpenSSH - 2 -](#_Toc55232469)

[Configurer et installer sur intel - 4 -](#_Toc55232470)

[Configurer et installer sur Nano Pi - 6 -](#_Toc55232471)

[Création de clefs - 7 -](#_Toc55232472)

[Configuration sshd - 7 -](#_Toc55232473)

[Test final - 8 -](#_Toc55232474)

[Modification des sources - 10 -](#_Toc55232475)

[Conclusion SSHD - 10 -](#_Toc55232476)

[Annexes - 11 -](#_Toc55232477)

# Introduction

Ce rapport est composé de trois laboratoires distincts :

1. SSHD
2. FileSystem
3. Firewall

# SSHD

## Introduction

Durant ce laboratoire nous allons principalement nous familiariser avec le protocole SSH et les utilitaires OpenSSH. SSH est protocole de connexion qui impose un échange de clés de chiffrement en début de connexion. Le port utilisé par défaut est le 22. OpenSSH est un ensemble d’outils open source utilisant le protocole SSH.

Durant ce laboratoire, plusieurs étapes nous a été demandé :

1. Installer et vérifier la signature d’OpenSSH
2. Configurer les packages sur notre machine Intel.
3. Configurer les packages sur la cible Nani Pi
4. Installer les différents utilitaires sur la cible.
5. Configurer des options de SSHD.
6. Modifier SSHD afin de ne plus indiquer la version utilisée.

## Installer et vérifier la signature d’OpenSSH

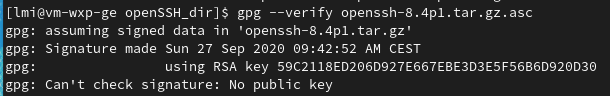
Afin d’installer OpenSSH il a fallu se rendre sur son site officiel (<https://www.openssh.com/>) et récupérer le lien http Suisse afin d’installer la dernière version :

*Wget https://mirror.ungleich.ch/pub/OpenBSD/OpenSSH/portable/*[*openssh-8.4p1.tar.gz*](https://mirror.ungleich.ch/pub/OpenBSD/OpenSSH/portable/openssh-8.4p1.tar.gz)

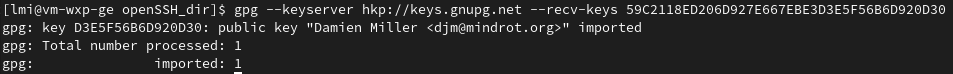
Dans le même temps, on peut télécharger la signature de celui-ci :

*Wget https://mirror.ungleich.ch/pub/OpenBSD/OpenSSH/portable/*[*openssh-8.4p1.tar.gz.asc*](https://mirror.ungleich.ch/pub/OpenBSD/OpenSSH/portable/openssh-8.4p1.tar.gz.asc)

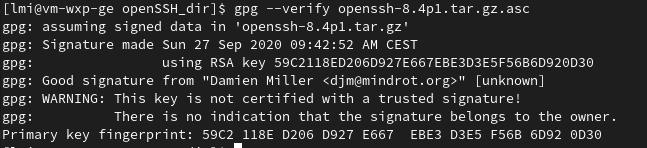
Pour commencer, il est important de vérifier l’authenticité et l’intégrité du logiciel :



On peut voir que le check n’est pas possible car la clef public n’est pas présente. Il faut importer cette clef sur notre PC comme suit :



On peut voir que la clef public de Damien Millet a correctement été importée. Il est maintenant possible de vérifier la signature du package :



## Configurer et installer sur intel

Maintenant que nous avons téléchargé OpenSSH, nous pouvons le configurer et l’installer sur notre machine hôte. Voici la commande à exécuter :

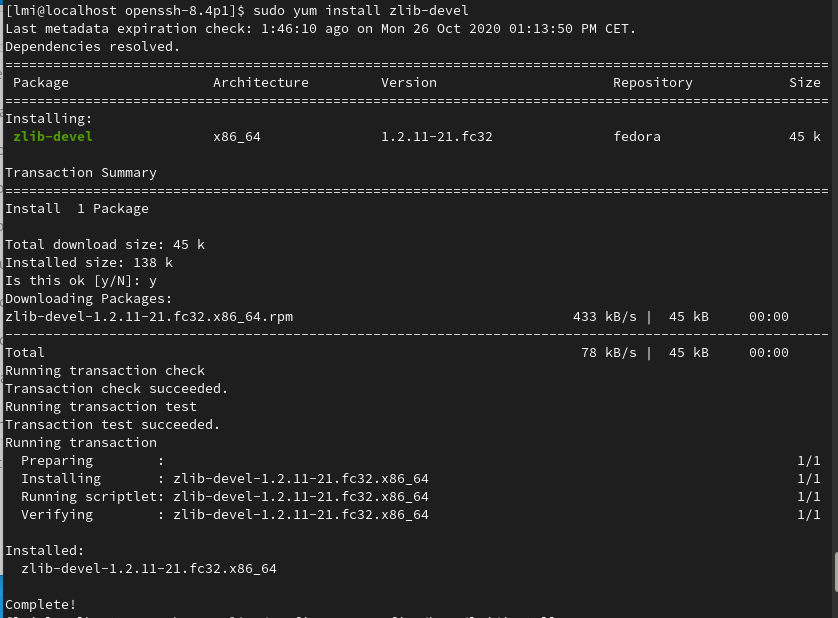
*./configure --prefix=/home/lmi/install*

L’option « –prefix » permet de modifier le répertoire d’installations.

Personnellement, j’ai eu l’erreur suivante :



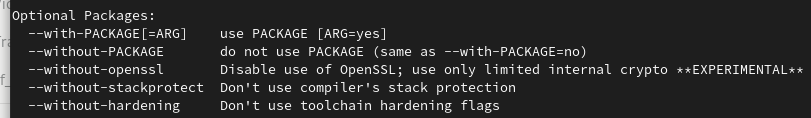
La librairie « zlib » n’est pas présente. Donc, je l’ai installée comme suit :



OpenSSH permet énormément de configuration et de différentes options, pour en savoir plus, il est intéressant de lire les fichiers « README » et « INSTALL ». Il est aussi possible d’utiliser la commande suivante :



Il nous est demandé d’activer l’option « hardening », cependant, grâce à la commande précédente, on peut apprendre que cette option est par défaut activée. Il est possible de la désactiver avec l’option « --without-hardening ».



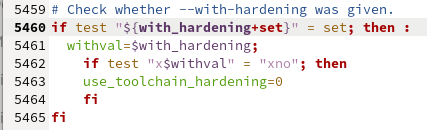
En m’intéressant aux différentes options proposées, j’ai pu voir celle-ci :



Il aurait été possible d’ajouter cette option dès le début afin de ne pas dépendre de la libraire « zlib ».

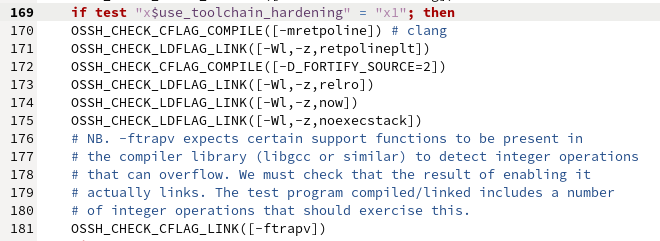
Afin de mieux comprendre l’impact de l’option « hardening », j’ai effectué une recherche de cette option et de son influence. Voici ce que j’ai pu trouver :

1. Dans le fichier « configure » :

7

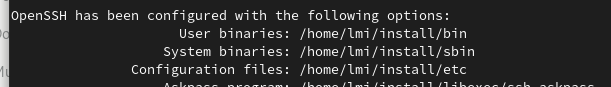
On peut voir que si l’option « hardening » activera, ou pas, la variable « use\_toolchain\_hardening ».

1. Dans le fichier « configure.ac » :



Dans le cas où cette même variable est active, cela va ajouter plusieurs option de compilation de protection listées ci-dessus.

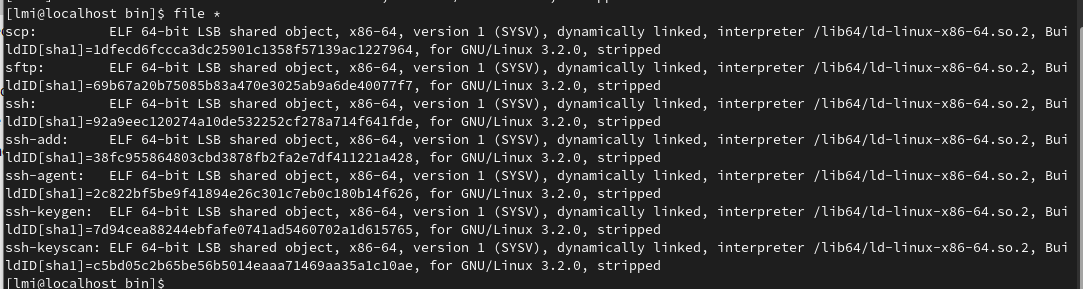
Une fois la configuration effectuée, un message résumant les informations de configuration son affichée :

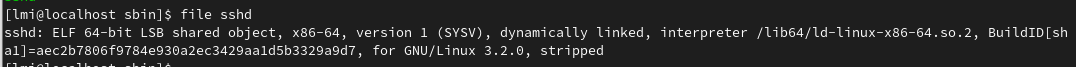


Ensuite, il est possible d’effectuer la compilation et l’installation avec les commandes suivantes :



Une fois tous les exécutables générés, il est possible de vérifier s’ils sont « stripped » :





On peut constater que tous les exécutables sont bien « stripped ».

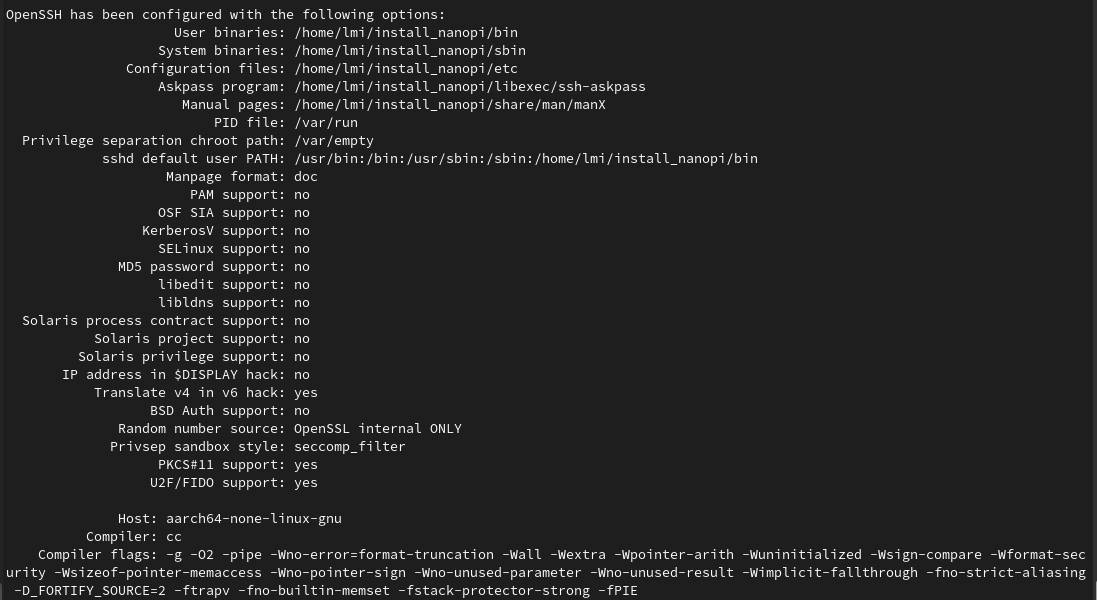
## Configurer et installer sur Nano Pi

L’objectif de cette étape est de configurer et installer OpenSSH sur la cible Nani Pi en utilisant la cross-compilation.

Étant donné cet utilitaire est relativement bien fait, il est facile de le cross-compiler. Il suffit d’ajouter une option lors de la configuration des packages. On peut voir la commande exécutée ci-dessous :

*./configure --host=aarch64-none-linux-gnu --prefix=/home/lmi/install\_nanopi*

On peut voir ci-dessous la sortie de la configuration. On peut voir en bas tous les flags de compilation activés.

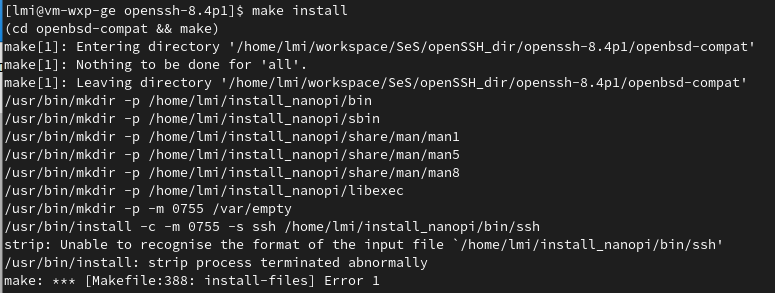


Ensuite, les deux commandes de compilation et d’installation peuvent être exécutées :

*make*

*make install*

Dans mon cas, la commande « make install » provoque une erreur :



La commande « strip » effectuée dans le script « /usr/bin/install » provoque une erreur. En faisant une recherche, voici ce que j’ai pu trouver :



On peut voir que la commande « strip » executée est celle par défaut avec un flag « -s ». Cependant, comme nous cross-compilons, il est nécessaire d’indiquer la commande « strip » pour notre architecture grâce au flag « --strip-program » :



Après cela, l’installation a pu se faire correctement.

Une fois que tous les fichiers exécutables sont correctement générés pour notre cible, il suffit de les placer sur le système de fichier de la Nano PI. Il y a plusieurs manières de procéder, pour ma part, j’ai utilisé le système de fichier réseau (NFS) préalablement installé.

## Création de clefs

L’objectif est de créer différents types de clef sur la cible à l’aide de l’utilitaire « ssh-keygen » précédemment installé. Voici ci-dessous la liste des différents type de clef crées et les commandes permettant leur création :

1. rsa 4096 bits



1. dsa 1024 bits



1. ecdsa 521 bits



1. ed25519 256bits



## Configuration sshd

La configuration SSHD se fera via le fichier « sshd\_config ». Afin de répondre aux configurations demandées, voici les lignes à ajouter au fichier :

**Utilisation uniquement de IPv4 :**

AddressFamily inet

**Ne pas permettre la redirection de port :**

AllowTcpForwarding no

AllowStreamLocalForwarding no

GatewayPorts no

PermitTunnel no

**Autoriser des algorithmes de chiffrement de hachage :**

Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes256-cbc

MACs hmac-sha1,hmac-sha2-256

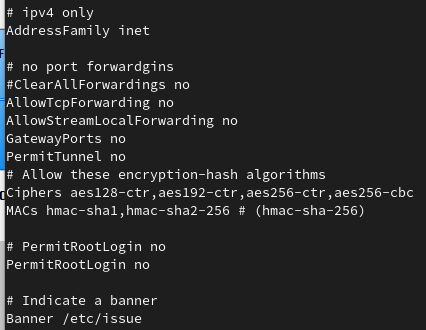
**Connexion root pas permis :**

PermitRootLogin no

**Indiquer une bannière :**

Banner /etc/issue

Voici plus précisément le fichier de configuration « sshd\_config ».



## Test final

L’objectif maintenant est de tester l’outil sshd sur la cile.

Afin de contrôler si un service ssh est en cours, on peut utiliser la commande « netstat -atu » afin de vérifier les programmes qui écoute les ports. Ensuite, il faut désactiver le service ssh en cours par défaut avec la commande « /etc/init.d/S50dropbear stop ».

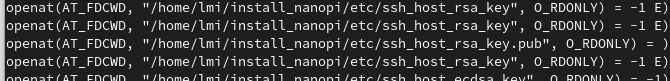
Afin de lancer le programme sshd précédemment configuré et installé, voici la commande à effectuer tout en précisant le fichier de configuration précédemment crée :



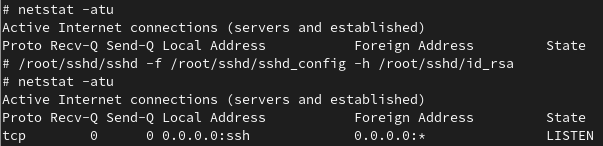
On peut remarquer qu’il nous indique qu’il ne dispose pas de clef hôte. Dans ce cas, il peut être intéressant d’utiliser la commande « strace » afin de mieux comprendre d’où vient le problème :



On peut voir ci-dessous que les clefs sont recherchées dans le dossier « /home/install\_nanopi/etc/ » :

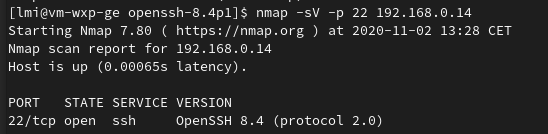


Il existe plusieurs façons d’indiquer l’emplacement des clefs. Personnellement, en analysant les paramètres possible au programme sshd, j’ai pu remarquer que l’option -h permet ceci. On peut voir ci-dessous la lancement de sshd en indiquant la clef rsa :



Grâce à la commande « netstat -atu », j’ai pu confirmer que le programme sshd c’était correctement lancé.

## Modification des sources



## Conclusion SSHD

Ce laboratoire m’a permis de comprendre les principes et le fonctionnement des clefs et des signatures dans le domaine de la sécurité. De plus, il m’a fait prendre conscience que la cross-compilation pouvait rapidement être complexe. J’ai pu accroitre ma connaissance en ce qui concerne la configuration du protocole SSH et des packages en général. Finalement, j’ai pu découvrir quelques commandes pratiques tels que « strace » et « netstat ».

# File system

## Introduction

Durant ce laboratoire nous allons principalement nous familiariser avec ; la manipulation de partitions, de différents systèmes de fichier, du cryptage de partition et de l’utilisation d’un initramfs.

Ce laboratoire est composé de plusieurs étapes distinctes :

1. Kernel and rootfs configuration
2. EXT4
3. Btrfs, f2fs, nilfs2 et xfs
4. LUKS, cryptsetup et dmcrypt
5. initramfs
6. initramfs-LUKS partition

## Kernel and rootfs configuration

Ce chapitre permet de configurer le noyau et le rootfs grâce à l’interface menu-config. Plusieurs configurations ont été ajoutées :

1. mkfs.ext2 (busybox-menuconfig)
2. tune2fs (busybox-menuconfig)
3. Btrfs, NILFS2, F2FS, XFS (linux-menuconfig)
4. USB Mass Storage (linux-menuconfig)
5. Cryptsetup (buildroot et linux-menuconfig)
6. Initramfs (linux-menuconfig)

Toutes ces étapes de configurations sont détaillées dans la donnée du laboratoire en annexe [1].

Une fois que la nouvelle configuration est terminée, il faut générer et installer le nouveau kernel et rootfs sur la carte SD. Par exemple, en utilisant un script créé lors des laboratoires précédent.

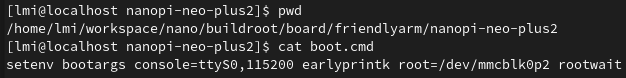
Typiquement, on peut vérifier que le package « cryptsetup » est disponible sur la cible NanoPi :



## EXT4

### Comment le noyau sait que le rootfs est sur la deuxième partition de la carte SD ?

Car on l’indique dans les arguments avant de lancer le noyau avec la commande « setenv » dans le fichier « boot.cmd ». Ce fichier se trouve dans le répertoire associé à la board utilisée. On peut voir plus précisément cette ligne de commande ci-dessous :



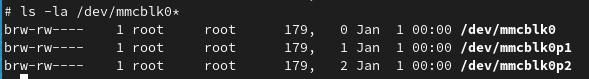
### Comment monter la première partition de la carte SD sur /mtn ?

On peut voir dans l’image ci-dessous comment monter la première partition de la carte sur un répertoire (/mnt) :

### 

### Quel est le numéro majeur et mineur du fichier nœud gérant la carte SD ?

On peut voir ci-dessous trois différents nœuds qui gère la carte SD :



La numéro majeur indiquant le driver utilisé est le 179. Ensuite les numéro mineurs se suivent simplement de 0 à 2.

## btrfs, f2fs, nilfs2, xfs

### Créer deux nouvelles partitions (3 et 4)

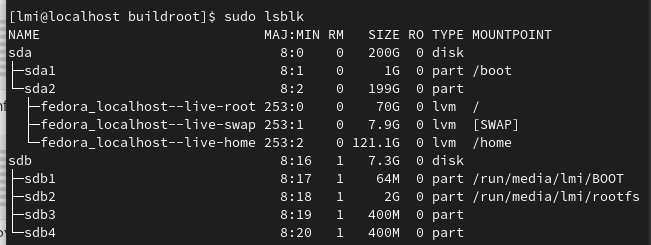
Voici les commandes que j’ai utilisées :

*sudo parted /dev/sdb mkpart primary ext4 4358144s 5177343s*

*sudo parted /dev/sdb mkpart primary ext4 5177344s 5996543s*

Le début en secteur (s) de la première partition créée est 4358144, qui est la suite (+1) de la fin de la partition précédant. Ensuite, il faut indiquer la fin de la partition en secteur. Afin de faire une partition de 400MB il faut ajouter 819 199 (Taille de la partition / Taille d’un secteur – 1 = 400MB / 512 - 1). Nous trouvons donc 5177343s. Le principe est le même pour la quatrième partition.

Il est de bonne habitude de vérifier le bon fonctionnement des commandes exécutées :



### Formater ces deux nouvelles partitions avec deux différents systèmes de fichier (btrfs et f2fs)

Personnellement j’ai choisi les système de fichier btrfs et f2fs. Voici les commandes que j’ai dû exécuter pour formater la troisième partition en f2fs :

*sudo dnf install f2fs-tools.x86\_64*

*sudo mkfs.f2fs -l usr\_f2fs /dev/sdb3*

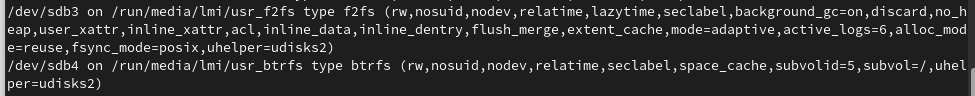
Voici celles pour formater la quatrième partition en btrfs :

*sudo dnf install btrfs-progs.x86\_64*

*sudo mkfs.btrfs /dev/sdb4*

*sudo btrfs filesystem label /dev/sdb4 usr\_btrfs*

Encore une fois, on peut contrôler le bon fonctionnement des commandes précédentes :



### Comparer les temps d’écriture entre les différents systèmes de fichier

Il peut arriver que le programme soit gêné par d’autres processus lors de la mesure. De ce fait, j’ai fait plusieurs mesures afin d’avoir une vision plus générale. Voici les différentes mesures observées lors des tests :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **btrfs** | | **ext4** | | **f2fs** | |
| small file | big file | small file | big file | small file | big file |
| **Mesures [ms]** | 65 | 36 | 13 | 8 | 16 | 6 |
| 58 | 10 | 18 | 10 | 14 | 6 |
| 54 | 527 | 17 | 10 | 19 | 8 |
| 67 | 13 | 14 | 6 | 12 | 9 |
| 102 | 1044 | 12 | 8 | 14 | 6 |
| 108 | 7 | 22 | 8 | 679 | 6 |
| 103 | 6 | 16 | 9 | 15 | 6 |
| 39 | 56 | 14 | 8 | 15 | 9 |
| 58 | 506 | 17 | 8 | 13 | 8 |
| 82 | 10 | 13 | 8 | 12 | 8 |
| 54 | 209 | 19 | 8 | 12 | 6 |
| 63 | 15 | 23 | 9 | 11 | 6 |
| **Moyenne** | 71.08 | 203.25 | 16.50 | 8.33 | 69.33 | 7.00 |
| **Médiane** | **64.00** | **25.50** | 16.50 | 8.00 | **14.00** | **6.00** |

On peut voir des mesures en rouge qui sont surement dû à des processus gênant lors de la mesure. Pour éviter de prendre en considération ce genre de mesures, la médiane a été privilégiée pour faire les comparaisons.

On peut constater que de manière générale le système de fichier offrant l’écriture la plus rapide est f2fs, suivit de ext4. Le système de fichier btrfs offre l’écriture la moins rapide.

*Remarque : Afin d’avoir facilement accès aux trois partitions, j’ai créé et exécutée mon programme C dans le même répertoire d’accès : « /run/media/lmi ». Mon programme prenait un deuxième argument indiquant le chemin du répertoire où créer les fichiers (Ex : «./usr\_f2fs/test\_writing »). Malheureusement, en redémarrant ma machine virtuelle mon code source était introuvable. Je pense que c’était une mauvaise idée de travail dans un répertoire permettant le montage de disque externe. En effet, après un second test, j’ai pu confirmer que le répertoire /run/media/lmi était supprimé après un redémarrage.*

## LUKS, cryptsetup et dmcrypt

### Créer une troisième partition LUKS

Pour commencer, j’ai créé la troisième partition :

*sudo parted /dev/sdb mkpart primary ext4 4358144s 6455295s*

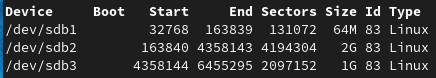
Le début en secteur (s) de la première partition créée est 4358144, qui est la suite (+1) de la fin de la partition précédant. Ensuite, il faut indiquer la fin de la partition en secteur. Afin de faire une partition de 1GB il faut ajouter *2 097 151* (Taille de la partition / Taille d’un secteur – 1 = 1GB / 512 - 1). Nous trouvons donc *6455295*s.

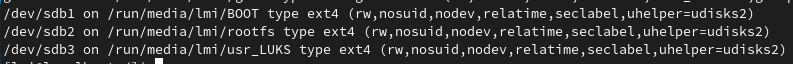
Ensuite, j’ai formaté la partition en ext4 :

*umount /dev/sdb3*

*sudo mkfs.ext4 /dev/sdb3 -L usr\_LUKS*

On peut vérifier le bon déroulement des commandes :





### LUKS, cryptsetup options

1. « Plain Mode » vs « LUKS extension mode » : La différence est que LUKS utilise un en-tête de métadonnées et peut donc offrir plus de fonctionnalités que dm-crypt (Plain Mode). D'autre part, la tête est visible et vulnérable aux dommages. À moins de très bien comprendre les contextes de cryptographie, il est en général conseillé d’utiliser LUKS.
2. *–hash* permet de remplacer la fonction de hachage par défaut pour le hachage de phrase de passe (passphrase).
3. La valeur par défaut actuelle dans les sources distribuées pour le chiffrement "aes-xts-plain64" pour LUKS.
4. *--key-file* permet principalement de fournir le passphrase par un fichier.

### LUKS test 1

***Initialiser une partition LUKS en format ext4 et la monter dans le répertoire /mtn/usr***

Voici la suite de commande effectuées :

*umount /dev/sdb3*

*sudo cryptsetup --debug --pbkdf-memory 256 luksFormat /dev/sdb3 (isaia test)*

*sudo cryptsetup --debug open --type luks /dev/sdb3 luks\_test*

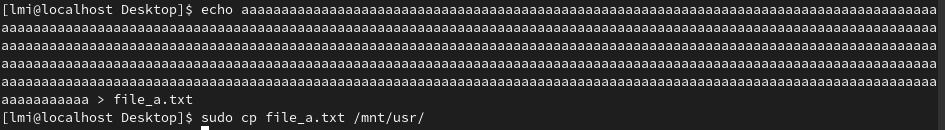


*sudo mkfs.ext4 /dev/mapper/luks\_test*

*sudo mkdir /mnt/usr*

*sudo mount /dev/mapper/luks\_test /mnt/usr/*

***Copier un fichier dans la partition LUKS***

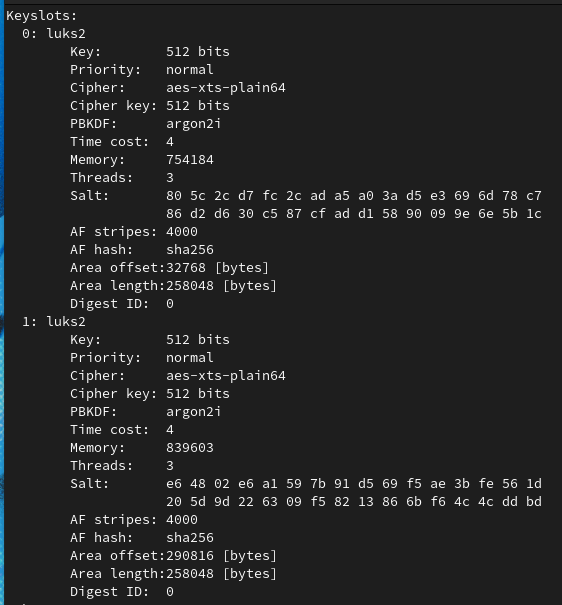


***Ajouter un nouveau passphrase à la partition LUKS***

Pour ce faire, il suffit d’utiliser la commande suivante :

*sudo cryptsetup luksAddKey /dev/sdb3*

Il est possible de vérifier qu’une second clef a été ajoutées en regardant l’en-tête du device LUKS avec cette commande : « sudo cryptsetup luksDump /dev/sdb3 » :

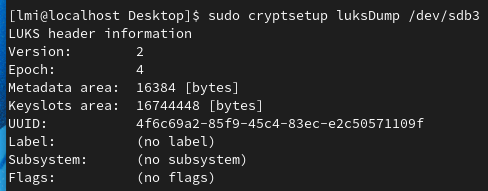


0

***Dump l’en-tête de la partition et la clé principale cryptée***

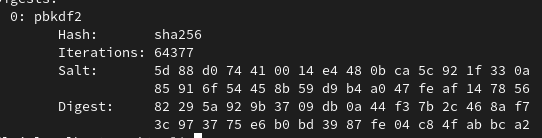
Comme nous l’avons fait précédemment, vois la commande our afficher l’entête de la partition :

*sudo cryptsetup luksDump /dev/sdb3*



Il est aussi possible d’utiliser cette commande afin d’afficher la clé principale cryptée :

*sudo cryptsetup luksDump -dump-master-key /dev/sdb3*

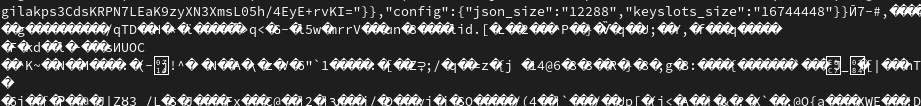


***Dump 1 Mbytes de la partition /dev/sbd3 sur un fichier. Peut-on trouver l’en-tête de la partition et le clé principale cryptée ? (aaaaaa ?)***

Voici comment j’ai fait pour dumper et afficher la troisième partition :



On peut constater que nous avons accès à l’en-tête de la partition ainsi qu’à la clé principale cryptée. La suite du fichier est complétement un indéchiffrable alors qu’il contient le fichier, précédemment inséré, avec beaucoup de caractères ‘a’ :



Après utilisation, il ne faut pas oublier de libérer les ressources :

*sudo umount /dev/mapper/luks\_test*

*sudo cryptsetup close luks\_test*

***Activer la partition cryptée sur la NanoPi***

Voici la suite de commande effectuées afin de pouvoir utiliser la partition cryptée sur la cible NanoPi :

*cryptsetup --debug open --type luks /dev/mmcblk0p3 usr\_luks*



*mkfs.ext2 /dev/mapper/usr\_luks*

*mkdir /mnt/usrfs*

*mount /dev/mapper/usr\_luks /mnt/usrfs/*

Maintenant il est possible d’utiliser la partition cryptée via /mnt/usrfs

Après utilisation, il ne faut pas oublier de libérer les ressources :

*umount /dev/mapper/usr\_luks*

*cryptsetup close usr\_luks*

### rootfs dans une partition LUKS

Le but de ce chapitre est d’avoir un rootfs crypté sur la partition 3.

***Générer un passphrase aléatoire dans un fichier***

*dd if=/dev/urandom of=file\_passphare bs=1 count=64*



***Initialise une partition LUKS sur la partition 3***

*sudo cryptsetup --debug --pbkdf-memory 256 --hash sha512 --key-size 512 --key-file ./file\_passphare luksFormat /dev/sdb3*

***Créer un mapping /dev/mapper/usrfs1***

*sudo cryptsetup --key-size 512 --key-file ./file\_passphare --debug open --type luks /dev/sdb3 rootfs\_luks*



***Formater la partition LUKS en format ext4***

*sudo mkfs.ext4 /dev/mapper/rootfs\_luks*

***Copier le rootfs sur la partition LUKS***

sudo dd if=~/workspace/nano/buildroot/output/images/rootfs.ext4 of=/dev/mapper/rootfs\_luks bs=4M

***Démarrer la NanoPi et monter manuellement la partition LUKS***

Premièrement, il est nécessaire d’avoir le fichier contenant le passphare aléatoire créé précédemment. Pour ce faire, j’ai utilisé le nfs afin de transmettre le fichier « file\_passphare » à la cible NanoPi.

Ensuite, j’ai créé un device afin d’avoir accès à la partition encryptée :

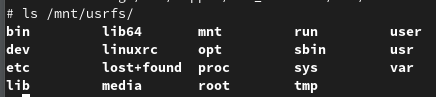
*cryptsetup --debug --key-size 512 --key-file ./file\_passphare open --type luks /dev/mmcblk0p3 usr\_luks*



Puis, j’ai monté la partition LUKS contenant le rootfs sur le répertoire /mnt/usrfs :

*mkdir /mnt/usrfs*

*mount /dev/mapper/usr\_luks /mnt/usrfs*



***Écrire un script (/etc/init.d/S40luks) afin de monter automatiquement la partition***

### initramfs

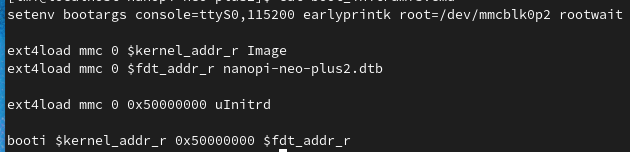
***Générer un initramfs***

Afin de générer un initramfs, j’ai suivi les directives données dans le document « File Systems, LUKS, InitRamFS » du cours Ses. Finalement, la création d’un script permettant de construire complètement l’initramfs est créé. Ce script est disponible dans les annexes [2].

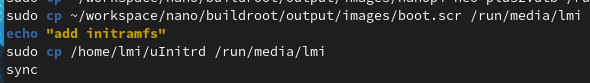
Il est intéressant d’exécuter la commande « tree /home/lmi/ramfs/ » afin de s’assurer que tous les répertoires, devices, libraires, exécutables et scripts soient correctement créent.

***Initialiser la NanoPi afin de démarrer l’initramfs***

Il est nécessaire de modifier le fichier « boot.cmd » correspondant à notre carte (~/workspace/nano/buildroot/board/friendlyarm/nanopi-neo-plus2/boot.cmd) afin de charger l’initramfs fraichement créé à une adresse disponible (0x5000 0000). De plus, il faut indiquer cette adresse grâce au deuxième argument de la commande « booti » :



Il ne faut pas oublier de modifier notre script qui permet de générer notre carte SD afin d’ajouter l’initramfs sur la partition 1 (BOOT).



***Démarre la NanoPi et démarre manuellement***

***Depuis le shell sur l’initramfs, monter la partition LUKS***

***Démarrer manuellement la partition roofs encryptée***

***Écrire un scrpit afin de démarrer automatiquement la partition rootfs encryptée.***

# Annexes

1. Donnée laboratoire « FileSystem »
2. Scirpt de construiction d’un initramfs

Date : x.yxx.20

Nom de l’étudiant : Spinelli Isaia