



# AUDIT DE SÉCURITÉ

## AUDIT DE SÉCURITÉ - FREELANCE - PROJET ALPHA

---

**Auditeur :** Guihot Romain - Administrateur Systèmes, Réseaux & Architectures Cloud

---

**Destinataire :** Mr Elon Musk - CEO SpaceX

---

**Mission :** Dans le cadre d'un audit de sécurité, remonter les problèmes signalés et faire des préconisations d'améliorations sans mettre en œuvre les corrections ou améliorations préconisées. Si le client décide de suivre les recommandations, leur mise en œuvre fera l'objet d'une mission distincte.

---

**Date de l'audit :** 04/07/2020

---

**Coût du projet :** 3000€ TTC

---

**Résultats :**  
Nombre de recommandations **TOTALE** : 58  
Nombre de recommandations **CRITIQUE** : 39  
Nombre de recommandations **ATTENTION** : 19

---

**Conclusion :** De nombreux vecteurs liés à la sécurité du serveur web ne sont pas mis en place et nécessitent une correction impérative. Veuillez trouver en page 41 le tableau de synthèse pour l'audit de sécurité du serveur Linux de distribution Ubuntu.

---

# SOMMAIRE - PLAN D'ACTION DE L'AUDIT

## A - Définition du périmètre de l'audit

- 1 - Enquête Forensic
- 2 - Le principe de minimisation
- 3 - Le principe de moindre privilège
- 4 - Le principe de défense en profondeur

## B - Réalisation technique de l'audit

- 1 - Analyse externe
- 2 - Mise en place de l'analyse Forensic
  - a) L'intégrité et la mise à jour des packages installés
- 3 - Auditer le processus de démarrage Grub
  - a) Bootloader, les options du noyau et ses modules
  - b) Les consoles virtuelles
  - c) Le mode de démarrage du serveur
- 4 - Auditer le système
  - a) Les composants matériels
  - b) Le partitionnement des disques
  - c) Les comptes utilisateurs, les mots de passes, les droits spéciaux et les mises à jours de sécurité
  - d) La configuration des services lancés
  - e) Le cloisonnement des services lancés
  - f) Les fichiers de trace des services
- 5 - Auditer les accès réseaux

- a) Les ports ouverts du serveur et les processus associés
- d) Les processus de filtrage réseau, pare feu et proxy
- e) Les services ssh et ftp

## C - Approfondir avec un logiciel d'audit

1 - Lynis

## D - Rapport d'audit et préconisations

1 - Tableaux du bilan d'audit & recommandations

2 - Préconisations additionnelles

- a) Politique de sécurité du SI au sein de l'entreprise
- b) Maîtriser les risques juridiques liés au numérique
- c) Mettre en place une veille en cybersécurité

---

## A - Définition du périmètre de l'audit

Afin d'auditer un système d'exploitation Linux sous distribution Debian dont le rôle est un serveur Web d'entreprise, nous allons définir les 4 grands principes de sécurité : **Enquête Forensic, Minimisation, Moindre privilège, Défense en profondeur.**



Ces principes sont décrits notamment en introduction du guide de recommandations de **l'ANSSI, l'agence nationale de la sécurité des systèmes d'information.**

## 1 - Enquête Forensic

Le principe d'une **enquête forensic** est de matérialiser les preuves informatiques et de retracer avec précision le mode opératoire de l'attaquant, l'origine de la compromission et le préjudice causé par cette dernière. **Dans notre cas, cette étude post intrusion sera réalisé de façon à vérifier l'hypothèse d'une attaque afin de garantir l'intégrité de l'audit de sécurité ainsi que les préconisations recommandées.**

- **Machine saine.** L'analyse Forensic indique aucune trace ou compromission par un attaquant
- **Machine Compromise.** L'analyse Forensic remonte des preuves d'une ou plusieurs intrusions, la corruption de certains services ou données.

## 2 - Le principe de minimisation

Le principe de **minimisation** consiste à étudier, après l'installation du serveur, l'ensemble des services et processus installés et configurés par défaut afin de les maîtriser. Cette étude permet notamment de :

- **réduire la surface d'attaque potentielle du serveur.** Par exemple, un service SMTP qui s'exécute inutilement est une cible potentielle d'attaque ;
- **réduire le nombre de composants exploités au strict minimum** pour assurer les tâches de mise à jour de manière optimale ;
- **permettre la mise en place d'une supervision efficace** et probante sur un nombre réduit et maîtrisé de composants.

Au delà de l'aspect sécurité, la minimisation permet d'optimiser les performances du serveur et de réduire sa consommation d'énergie.

### 3 - Le principe de moindre privilège

Le principe de **moindre privilège** consiste à s'assurer que tous les objets gérés par le système d'exploitation (processus, fichiers, etc.) disposent uniquement des droits nécessaires à leur fonction. Rien de plus.

- **lecture** : la ressource peut être lue ou chargée en mémoire ;
- **écriture** : la ressource peut être créée ou modifiée ;
- **exécution** : la ressource peut être exécutée en tant que programme.

Les objectifs de cette démarche de moindre privilège sont avant tout de :

- s'assurer qu'un processus qui sort de son périmètre fonctionnel classique (par anomalie technique ou par malveillance volontaire) soit le moins nocif possible, car contraint par des **droits d'accès bien gérés** ;
- s'assurer qu'il n'est pas possible d'effectuer des actions dangereuses pour le système sans disposer de **privilèges élevés**, qui ne sont pas simples à acquérir (protection par mot de passe fort, fichiers de trace, etc.).

### 4 - Le principe de défense en profondeur

Le principe de **défense en profondeur** implique d'ajouter autant de barrières de sécurité possibles afin de retarder au maximum la prise de contrôle du serveur ou l'accès à la donnée lors d'une attaque.

Concrètement, ce principe va le plus souvent résulter en :

- **Cloisonnement** des **services réseaux** ( VLAN, Parefeu & Séparer les composants applicatifs )
  - un serveur frontal (Apache par exemple) ;
  - un serveur pour l'application (Tomcat par exemple) ;
  - un serveur pour la base de données (MySQL par exemple).
- la mise en place d'un **processus d'authentification manuel obligatoire** pour toute action privilégiée ;
- la mise en place d'une **gestion centralisée et sécurisée des traces** (journaux d'évènements applicatifs ou système) ;
- la mise en place d'un **système de supervision** avec gestion d'alerte afin de détecter très rapidement les tentatives de compromission
- un **cloisonnement systématique des processus exposés**.

# B - Réalisation technique de l'audit

## 1 - Analyse Externe

```
nmap -T4 -A -v 192.168.43.246
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-21 16:05 Paris, Madrid (heure d'été)
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:05
Completed NSE at 16:05, 0.00s elapsed
Initiating NSE at 16:05
Completed NSE at 16:05, 0.00s elapsed
Initiating NSE at 16:05
Completed NSE at 16:05, 0.00s elapsed
Initiating ARP Ping Scan at 16:05
Scanning 192.168.43.246 [1 port]
Completed ARP Ping Scan at 16:05, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:05
Completed Parallel DNS resolution of 1 host. at 16:05, 0.00s elapsed
Initiating SYN Stealth Scan at 16:05
Scanning vm-audit (192.168.43.246) [1000 ports]
Discovered open port 25/tcp on 192.168.43.246
Discovered open port 80/tcp on 192.168.43.246
Discovered open port 22/tcp on 192.168.43.246
Discovered open port 3306/tcp on 192.168.43.246
Discovered open port 53/tcp on 192.168.43.246
Discovered open port 143/tcp on 192.168.43.246
Discovered open port 110/tcp on 192.168.43.246
Completed SYN Stealth Scan at 16:05, 0.01s elapsed (1000 total ports)
Initiating Service scan at 16:05
Scanning 7 services on vm-audit (192.168.43.246)
Completed Service scan at 16:05, 6.28s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against vm-audit (192.168.43.246)
NSE: Script scanning 192.168.43.246.
Initiating NSE at 16:05
Completed NSE at 16:05, 8.11s elapsed
Initiating NSE at 16:05
Completed NSE at 16:05, 0.08s elapsed
Initiating NSE at 16:05
Completed NSE at 16:05, 0.00s elapsed
Nmap scan report for vm-audit (192.168.43.246)
Host is up (0.00s latency).
Not shown: 993 closed ports
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 93:7e:24:45:35:50:f9:fa:6f:6d:96:21:3f:06:84:1e (RSA)
|_ 256 a1:ec:bf:a4:53:f8:10:55:11:92:b5:b2:bc:98:60:e0 (ECDSA)
|_ 256 16:49:88:88:48:a4:e7:da:ee:21:88:ad:14:2c:f6:fe (ED25519)
25/tcp    open  smtp      Postfix smtpd
|_ _smtp_commands: vm-audit, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ ssl-cert: Subject: commonName=vm-audit
|_ Issuer: commonName=vm-audit
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2018-07-03T13:52:46
|_ Not valid after: 2028-06-30T13:52:46
|_ MD5: 3215 45fc 0b4c 29d3 00d2 6e98 9ff2 c36d
|_ _SHA-1: 2565 1283 e8f3 cc95 1561 2f32 0373 4a10 78a4 c561
|_ _ssl_date: TLS randomness does not represent time
53/tcp    open  domain   ISC BIND 9.10.3-P4 (Ubuntu Linux)
|_ dns-nsid:
|_ _bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ _http_server_header: Apache/2.4.18 (Ubuntu)
|_ _http_title: Did not follow redirect to http://vm-audit:8080/
110/tcp   open  pop3      Dovecot pop3d
|_ _pop3_capabilities: RESP-CODES CAPA SASL PIPELINING UIDL TOP AUTH-RESP-CODE
143/tcp   open  imap      Dovecot imapd
|_ _imap_capabilities: SASL-IR more OK ENABLE post-login LITERAL+ LOGIN-REFERRALS IDLE capabilities have IMAP4rev1 ID listed Pre-login LOGINDISABLEDA0001
3306/tcp  open  mysql     MySQL (unauthorized)
```

Le scan réseau de la machine depuis l'extérieur montre qu'il existe deux vulnérabilités :

La première concerne la vulnérabilité de la base de donnée en ouverture depuis l'extérieur par le port 3306/tcp

**RECOMMANDATION-CRITICAL** (Défense en profondeur) : Interdire l'ouverture du port 3306 vers l'extérieur ( Sauf si un autre serveur Apache doit s'y connecter )

La seconde partie concerne l'affichage de chaque services ouverts comme le montre la capture ci-dessus : OpenSSH 7.2p2 ubuntu2.2 / Apache 2.4.18. Privilégier de mettre en "silence/caché" la version des services pour éviter les exploits.

**RECOMMANDATION-CRITICAL** (Défense en profondeur) : Cacher la version des services visibles depuis un scan réseau externe

## 2 - Mise en place de l'analyse Forensic

### a) L'intégrité et la mise à jour des packages installés

# Les distributions fournissent le système sous la forme de packages de sources précompilées. Cette fonctionnalité très pratique nous permet d'éviter de devoir compiler manuellement les composants du système. Cependant, il faut toujours vérifier que les éditeurs de distributions n'ont pas mis à jour un package suite à la publication d'une **CVE (Common Vulnerabilities Exposure)**. Pour effectuer cette veille de façon correcte, il faut s'assurer que les dépôts de packages interrogés sont qualifiés et sûrs.

Pour cela, il faut vérifier, dans les fichiers de configuration du **package manager**, que les adresses des dépôts pointent vers des serveurs maintenus directement par l'éditeur, et que les packages téléchargés comportent une signature numérique.

```
bigboss@vm-audit: /
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://fr.archive.ubuntu.com/ubuntu/ xenial universe
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial universe
deb http://fr.archive.ubuntu.com/ubuntu/ xenial-updates universe
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://fr.archive.ubuntu.com/ubuntu/ xenial multiverse
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial multiverse
deb http://fr.archive.ubuntu.com/ubuntu/ xenial-updates multiverse
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb http://fr.archive.ubuntu.com/ubuntu/ xenial-backports main restricted universe multiverse
# deb-src http://fr.archive.ubuntu.com/ubuntu/ xenial-backports main restricted universe multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu xenial partner
# deb-src http://archive.canonical.com/ubuntu xenial partner

deb http://security.ubuntu.com/ubuntu xenial-security main restricted
# deb-src http://security.ubuntu.com/ubuntu xenial-security main restricted
deb http://security.ubuntu.com/ubuntu xenial-security universe
# deb-src http://security.ubuntu.com/ubuntu xenial-security universe
deb http://security.ubuntu.com/ubuntu xenial-security multiverse
# deb-src http://security.ubuntu.com/ubuntu xenial-security multiverse
```

```

bigboss@vm-audit:/$ apt-key fingerprint
/etc/apt/trusted.gpg
-----
pub   1024D/437D05B5 2004-09-12
      Empreinte de la clef = 6302 39CC 130E 1A7F D81A 27B1 4097 6EAF 437D 05B5
uid   Ubuntu Archive Automatic Signing Key <ftpmaster@ubuntu.com>
sub   2048g/79164387 2004-09-12

pub   4096R/C0B21F32 2012-05-11
      Empreinte de la clef = 790B C727 7767 219C 42C8 6F93 3B4F E6AC C0B2 1F32
uid   Ubuntu Archive Automatic Signing Key (2012) <ftpmaster@ubuntu.com>

pub   4096R/EFE21092 2012-05-11
      Empreinte de la clef = 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092
uid   Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

pub   1024D/FBB75451 2004-12-30
      Empreinte de la clef = C598 6B4F 1257 FFA8 6632 CBA7 4618 1433 FBB7 5451
uid   Ubuntu CD Image Automatic Signing Key <cdimage@ubuntu.com>

```

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que l'ensemble des packages installés sur le système sont signés et sûrs avec les attributs **gpgcheck** et **gpgkey**

```

Ubuntu 16.04.3 LTS vm-audit tty1

vm-audit login: bigboss
Password:
Last login: Sun Jul 26 21:13:34 CEST 2020 from 192.168.43.95 on pts/0
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

313 paquets peuvent être mis à jour.
217 mises à jour de sécurité.

New release '18.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

```

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que l'ensemble des mises à jour de sécurités et dernières versions des packages sont installés.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier la planification régulière d'une tâche automatique pour mettre à jour les packages corrigés pour raisons de sécurité

### 3 - Auditer le processus de démarrage Grub

a) bootloader, les options du noyau et ses modules



```

bigboss@vm-audit:/$ ls -lrtha /etc/grub.d/
total 84K
-rwxr-xr-x  1 root root 6,2K janv. 24 2018 05_debian_theme
-rw-r--r--  1 root root 483 mars 21 2018 README
-rwxr-xr-x  1 root root 216 mars 21 2018 41_custom
-rwxr-xr-x  1 root root 214 mars 21 2018 40_custom
-rwxr-xr-x  1 root root 1,4K mars 21 2018 30_uefi-firmware
-rwxr-xr-x  1 root root 12K mars 21 2018 30_os-prober
-rwxr-xr-x  1 root root 11K mars 21 2018 20_linux_xen
-rwxr-xr-x  1 root root 13K mars 21 2018 10_linux
-rwxr-xr-x  1 root root 9,6K mars 21 2018 00_header
drwxr-xr-x  2 root root 4,0K juil. 3 2018 .
drwxr-xr-x 103 root root 4,0K juil. 14 13:50 ..
bigboss@vm-audit:/$ █

```

# Les fichiers appartiennent bien à l'utilisateur **root**, cependant les droits associés sont trop permissifs.

**RECOMMANDATION-CRITICAL** (moindre privilège) : passer les droits sur l'arborescence `/etc/grub.d/` à 700

# Le fichier **01\_users** est absent. Ce dernier est codifié pour contenir les informations d'authentification qui protègent l'accès au *shell* de Grub

**RECOMMANDATION-CRITICAL** (minimisation) : Créer un utilisateur et son mot de passe chiffré dans le fichier `01_users` afin de protéger l'accès au *shell* de Grub par une authentification

```

GNU nano 2.5.3 Fichier : /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
#GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=2
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT=""
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo`
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"

[ Lecture de 34 lignes (Attention : en lecture seule !) ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^T Orthograp.

```

# Lors de la vérification des options par défaut du noyau linux, en plus des options liées au partitionnement LVM et de celles liées à la configuration des variables d'environnement (langue, encodage), deux options sont absentes au noyau. **rhgb** et **quiet**. Ces deux options sont de l'ordre du confort pour l'utilisateur car elles présentent un écran graphique pendant le démarrage, cachant ainsi la plupart des messages du noyau pendant le processus.

**RECOMMANDATION-WARNING** (minimisation) : passer l'option **rhgb** et **quiet** aux variables GRUB\_CMD\_LINUX\_DEFAULT & GRUB\_CMD\_LINUX

# Dans le cadre de l'exploitation de systèmes virtualisés, il existe un service géré directement par le noyau Linux : **IOMMU**. Ce service permet de protéger la mémoire contre des accès non contrôlés, issus des périphériques du système. Par défaut, Linux gère IOMMU et va, selon le contexte, l'activer ou non. Il est recommandé de forcer l'activation de ce service en passant une option supplémentaire lors du démarrage du noyau.

**RECOMMANDATION-WARNING** (minimisation) : passer l'option **iommu=force** au noyau lors du démarrage de Linux

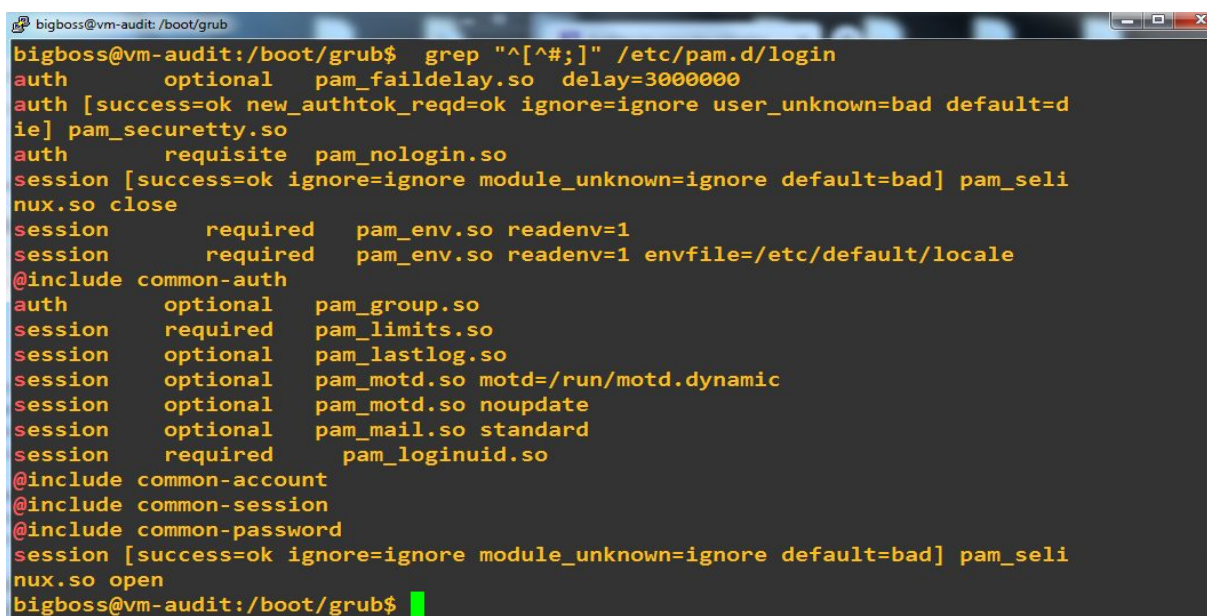


```
bigboss@vm-audit: /boot/grub
bigboss@vm-audit:/boot/grub$ sysctl kernel.modules_disabled
kernel.modules_disabled = 0
bigboss@vm-audit:/boot/grub$
```

# Il est possible de charger de manière dynamique de nouveaux modules sur le noyau actuel. Par défaut, cette variable est souvent positionnée à la valeur **0**, ce qui autorise le chargement à chaud de modules supplémentaires dans le noyau.

**RECOMMANDATION-WARNING** (minimisation) : Bloquer le chargement de modules supplémentaires via la `sysctl kernel.modules_disabled=1`. Veiller à intégrer les modules non dynamiquement par recompilation du noyau ( Attention aux serveurs applicatifs qui nécessitent de nouveaux modules )

## b) Les consoles virtuelles



```
bigboss@vm-audit: /boot/grub
bigboss@vm-audit:/boot/grub$ grep "^[^#;]" /etc/pam.d/login
auth optional pam_faildelay.so delay=3000000
auth [success=ok new_authok_reqd=ok ignore=ignore user_unknown=bad default=die] pam_securetty.so
auth requisite pam_nologin.so
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selnux.so close
session required pam_env.so readenv=1
session required pam_env.so readenv=1 envfile=/etc/default/locale
@include common-auth
auth optional pam_group.so
session required pam_limits.so
session optional pam_lastlog.so
session optional pam_motd.so motd=/run/motd.dynamic
session optional pam_motd.so noupdate
session optional pam_mail.so standard
session required pam_loginuid.so
@include common-account
@include common-session
@include common-password
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selnux.so open
bigboss@vm-audit:/boot/grub$
```

# Le fichier `/etc/securetty` du module `pam_securetty.so` contient la liste des terminaux sous la forme de périphériques (sans le `/dev/`), autorisant la connexion de l'utilisateur **root**. De nombreux terminaux autorisent cette connexion par défaut. La configuration actuelle présente donc une faille de sécurité.

Il est recommandé d'empêcher la connexion directe de l'utilisateur **root** depuis une console virtuelle. Mais il est tout à fait possible de se connecter avec un utilisateur moins privilégié pour ensuite passer sous l'utilisateur **root** avec la commande **su**.

**RECOMMANDATION-CRITICAL** (Défense en profondeur) : Videz le contenu `tty1` à `tty63` du fichier `/etc/securetty` afin de bloquer toute connexion avec l'utilisateur **root** depuis une console virtuelle

# Dans le fichier `/etc/securetty`, le module `pam_faildelay.so` traduit le temps d'attente par défaut entre deux tentatives de connexion suite à un échec. Ici la configuration est de 30 secondes.

**RECOMMANDATION-WARNING** (Défense en profondeur) : Augmenter l'intervalle de temps entre chaque tentative de connexion sur le module **pam\_faildelay.so** afin de ralentir les attaques par dictionnaire ( anti-robot)

# La combinaison de touches `Ctrl+Alt+Suppr` se traduit le plus souvent par un **ordre de redémarrage de la machine** ! Toute personne pouvant accéder au clavier peut redémarrer la machine avec cette combinaison de touches, ce qui n'est pas acceptable.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Désactivez la combinaison **Ctrl+Alt+Suppr** sur le serveur pour prévenir tout redémarrage depuis un accès physique à la machine

### c) Le mode de démarrage du serveur

```
bigboss@vm-audit:~$ systemctl get-default
graphical.target
bigboss@vm-audit:~$
```

# La cible du lancement de service par défaut est `graphical.target`. Pour cette machine cela n'est pas recommandé car aucun affichage graphique n'a été installé.

**RECOMMANDATION-WARNING** (minimisation) : Changer la cible par défaut avec un service non graphique : `multi-user.target`

```

bigboss@vm-audit:~$ systemctl list-units --type target
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
basic.target                        loaded active active Basic System
cryptsetup.target                  loaded active active Encrypted Volumes
getty.target                        loaded active active Login Prompts
graphical.target                   loaded active active Graphical Interface
local-fs-pre.target                loaded active active Local File Systems (Pre)
local-fs.target                    loaded active active Local File Systems
mail-transport-agent.target        loaded active active Mail Transport Agent
multi-user.target                  loaded active active Multi-User System
network-online.target              loaded active active Network is Online
network-pre.target                 loaded active active Network (Pre)
network.target                     loaded active active Network
nss-lookup.target                 loaded active active Host and Network Name Lookups
nss-user-lookup.target            loaded active active User and Group Name Lookups
paths.target                       loaded active active Paths
remote-fs-pre.target               loaded active active Remote File Systems (Pre)
remote-fs.target                   loaded active active Remote File Systems
slices.target                      loaded active active Slices
sockets.target                    loaded active active Sockets
sound.target                       loaded active active Sound Card
swap.target                        loaded active active Swap
sysinit.target                     loaded active active System Initialization
time-sync.target                  loaded active active System Time Synchronized
timers.target                      loaded active active Timers

LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB     = The low-level unit activation state, values depend on unit type.

23 loaded units listed. Pass --all to see loaded but inactive units, too.

```

# 23 unités cibles sont chargés au démarrage de linux. Certaines ne sont pas indispensables et limite donc la surface d'attaque potentiel.

**RECOMMANDATION-WARNING** (minimisation) : Supprimer les cibles inutiles comme sound.target & graphical.target ( Attention ce dernier doit être supprimé que si aucun GUI ne sera installé ) Si le serveur n'est pas un serveur de messagerie alors mail-transport-agent.target peut également être supprimé.

```

bigboss@vm-audit:~$ ls -lrtha /etc/systemd/system/graphical.target.wants/
total 8,0K
lrwxrwxrwx 1 root root 43 juil. 3 2018 accounts-daemon.service -> /lib/systemd/system/accounts-daemon.service
drwxr-xr-x 2 root root 4,0K juil. 3 2018 .
drwxr-xr-x 12 root root 4,0K juil. 3 2018 ..
bigboss@vm-audit:~$ ls -lrtha /etc/systemd/system/multi-user.target.wants/
total 8,0K
lrwxrwxrwx 1 root root 35 juil. 3 2018 rsyslog.service -> /lib/systemd/system/rsyslog.service
lrwxrwxrwx 1 root root 36 juil. 3 2018 remote-fs.target -> /lib/systemd/system/remote-fs.target
lrwxrwxrwx 1 root root 38 juil. 3 2018 networking.service -> /lib/systemd/system/networking.service
lrwxrwxrwx 1 root root 32 juil. 3 2018 cron.service -> /lib/systemd/system/cron.service
lrwxrwxrwx 1 root root 33 juil. 3 2018 lxcfs.service -> /lib/systemd/system/lxcfs.service
lrwxrwxrwx 1 root root 33 juil. 3 2018 mysql.service -> /lib/systemd/system/mysql.service
lrwxrwxrwx 1 root root 31 juil. 3 2018 ufw.service -> /lib/systemd/system/ufw.service
lrwxrwxrwx 1 root root 31 juil. 3 2018 atd.service -> /lib/systemd/system/atd.service
lrwxrwxrwx 1 root root 33 juil. 3 2018 bind9.service -> /lib/systemd/system/bind9.service
lrwxrwxrwx 1 root root 35 juil. 3 2018 dovecot.service -> /lib/systemd/system/dovecot.service
lrwxrwxrwx 1 root root 31 juil. 3 2018 ssh.service -> /lib/systemd/system/ssh.service
lrwxrwxrwx 1 root root 44 juil. 3 2018 snapd.autoimport.service -> /lib/systemd/system/snapd.autoimport.service
lrwxrwxrwx 1 root root 33 juil. 3 2018 snapd.service -> /lib/systemd/system/snapd.service
drwxr-xr-x 12 root root 4,0K juil. 3 2018 ..
lrwxrwxrwx 1 root root 41 juil. 3 2018 open-vm-tools.service -> /lib/systemd/system/open-vm-tools.service
lrwxrwxrwx 1 root root 47 juil. 3 2018 unattended-upgrades.service -> /lib/systemd/system/unattended-upgrades.service
lrwxrwxrwx 1 root root 42 juil. 3 2018 lxd-containers.service -> /lib/systemd/system/lxd-containers.service
lrwxrwxrwx 1 root root 36 juil. 4 2018 fail2ban.service -> /lib/systemd/system/fail2ban.service
drwxr-xr-x 2 root root 4,0K juil. 4 2018 .

```

```
bigboss@vm-audit: ~$ systemctl list-unit-files --type service --state enabled
UNIT FILE                                STATE
accounts-daemon.service                 enabled
atd.service                              enabled
autovt@.service                         enabled
bind9.service                           enabled
cron.service                            enabled
dovecot.service                         enabled
fail2ban.service                       enabled
friendly-recovery.service               enabled
getty@.service                          enabled
iscsi.service                           enabled
iscsid.service                          enabled
lvm2-monitor.service                   enabled
lxcfs.service                           enabled
lxd-containers.service                 enabled
mysql.service                           enabled
networking.service                     enabled
open-iscsi.service                     enabled
open-vm-tools.service                  enabled
resolvconf.service                     enabled
rsyslog.service                        enabled
snapd.autoimport.service               enabled
snapd.service                           enabled
snapd.system-shutdown.service          enabled
ssh.service                             enabled
sshd.service                            enabled
syslog.service                          enabled
systemd-timesyncd.service              enabled
ufw.service                             enabled
unattended-upgrades.service            enabled
ureadahead.service                     enabled
```

# La liste des fichiers du répertoire correspond à la liste des services qui se lancent automatiquement au démarrage de la machine

**RECOMMANDATION-CRITICAL** (minimisation) : Supprimer les services cibles inutiles démarrés automatiquement avec le serveur comme atd.service ( car cron.service déjà présent. dovecot.service ( uniquement si le serveur web n'utilise pas de service messagerie configurable avec imap/pop ) Ajouter accounts-daemon.service ( service chargé par défaut du graphical.target remplacé par multi-user.target )

## 4 - Auditer le système

### a) Les composants matériels

```
bigboss@vm-audit:~$ dmesg | grep CPU
[ 0.000000] CPU MTRRs all blank - virtualized system.
[ 0.000000] ACPI: SSDT 0x000000003FFF02A0 0001CC (v01 VBOX VBOXCPUT 00000002 INTL 20100528)
[ 0.000000] smpboot: Allowing 1 CPUs, 0 hotplug CPUs
[ 0.000000] setup_percpu: NR_CPUS:512 nr_cpumask_bits:512 nr_cpu_ids:1 nr_node_ids:1
[ 0.000000] PERCPU: Embedded 33 pages/cpu @ffff88003fc00000 s98264 r8192 d28712 u2097152
[ 0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[ 0.000000] RCU restricting CPUs from NR_CPUS=512 to nr_cpu_ids=1.
[ 0.064359] CPU: Physical Processor ID: 0
[ 0.065430] mce: CPU supports 0 MCE banks
[ 0.232942] smpboot: CPU0: Intel(R) Core(TM) i7-4810MQ CPU @ 2.80GHz (family: 0x6, model: 0x3c, stepping: 0x3)
[ 0.233603] Performance Events: unsupported p6 CPU model 60 no PMU driver, software events only.
[ 0.235010] x86: Booted up 1 node, 1 CPUs
[ 0.864663] ledtrig-cpu: registered to indicate activity on CPUs
[ 0.866445] microcode: CPU0 sig=0x306c3, pf=0x40, revision=0x0
bigboss@vm-audit:~$ grep ^flags /proc/cpuinfo | head -n1 | egrep --color=auto '
(pae|nx) '
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush mmx fxsr sse sse2 syscall nx rdtscp lm constant_tsc rep_good n
opl xtopology nonstop_tsc pni pclmulqdq monitor ssse3 cx16 sse4_1 sse4_2 x2apic
movbe popcnt aes xsave avx rdrand hypervisor lahf_lm abm
bigboss@vm-audit:~$
```

# Pour le processeur ce qui est important de remarquer, c'est la présence de **PAE** et **NX**. Ces deux attributs indiquent que le processeur protège l'exécution d'instructions stockées dans les régions mémoire non autorisées.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que le CPU dispose bien des flags PAE et NX

```
bigboss@vm-audit:~$ dmesg | grep Memory
[ 0.000000] Memory: 975720K/1048120K available (8474K kernel code, 1293K rwdata, 3984K rodata, 1488K init, 1316K bss, 72400K reserved, 0K cma-reserved)
bigboss@vm-audit:~$
```

# Pour la mémoire, le noyau laisse une trace de la quantité de mémoire requise au démarrage. A noter que cette valeur est susceptible d'augmenter ou de diminuer selon la compilation du noyau.

```
bigboss@vm-audit:~$ cat /proc/meminfo
MemTotal:          1016096 kB
MemFree:           226068 kB
MemAvailable:      611760 kB
Buffers:           16040 kB
Cached:            500864 kB
SwapCached:        0 kB
Active:            520764 kB
Inactive:          204284 kB
Active(anon):      183184 kB
Inactive(anon):    39680 kB
Active(file):      337580 kB
Inactive(file):    164604 kB
Unevictable:       3652 kB
Mlocked:           3652 kB
SwapTotal:         1044476 kB
SwapFree:          1044476 kB
Dirty:             0 kB
Writeback:         0 kB
AnonPages:         211828 kB
Mapped:            74604 kB
Shmem:             12300 kB
Slab:              36784 kB
SReclaimable:     22288 kB
SUnreclaim:       14496 kB
KernelStack:      2624 kB
PageTables:        7056 kB
NFS_Unstable:     0 kB
Bounce:           0 kB
WritebackTmp:     0 kB
CommitLimit:      1552524 kB
Committed_AS:     935508 kB
VmallocTotal:     34359738367 kB
VmallocUsed:       0 kB
VmallocChunk:     0 kB
HardwareCorrupted: 0 kB
AnonHugePages:    147456 kB
CmaTotal:          0 kB
CmaFree:           0 kB
```

# Il est également toujours important de conserver un minimum de SWAP, ne serait-ce que pour compenser un bug qui viendrait manger toute la mémoire vive... et ainsi éviter ainsi un crash du système. En effet, la mémoire SWAP permet d'ajouter au noyau un périphérique de type bloc (stocké sur le disque dur) pour écrire et lire les pages mémoire au cas où la mémoire vive serait saturée

**RECOMMANDATION-WARNING** (défense en profondeur) : Vérifier la présence d'un minimum de mémoire SWAP sur le système

## b) Le partitionnement des disques

```

bigboss@vm-audit:~$ sudo fdisk -l
Disque /dev/sda : 10 GiB, 10737418240 octets, 20971520 secteurs
Unités : sectors of 1 * 512 = 512 octets
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifiant: 0x13ba9979

Périphérique Amorçage Start Fin Secteurs Size Id Type
/dev/sda1 * 2048 999423 997376 487M 83 Linux
/dev/sda2 1001470 20969471 19968002 9,5G 5 Étendue
/dev/sda5 1001472 20969471 19968000 9,5G 8e LVM Linux

Disque /dev/mapper/vm--audit--vg-root : 6,5 GiB, 6924795904 octets, 13524992 secteurs
Unités : sectors of 1 * 512 = 512 octets
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disque /dev/mapper/vm--audit--vg-swap_1 : 1020 MiB, 1069547520 octets, 2088960 secteurs
Unités : sectors of 1 * 512 = 512 octets
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
bigboss@vm-audit:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 10G 0 disk
├─sda1 8:1 0 487M 0 part /boot
├─sda2 8:2 0 1K 0 part
├─sda5 8:5 0 9,5G 0 part
│   └─vm--audit--vg-root 252:0 0 6,5G 0 lvm /
│       └─vm--audit--vg-swap_1 252:1 0 1020M 0 lvm [SWAP]
sr0 11:0 1 1024M 0 rom
bigboss@vm-audit:~$

bigboss@vm-audit:~$ blkid /dev/sda5
/dev/sda5: UUID="BB0N16-QqFx-XxB1-eqjQ-fvCV-7r80-MxZxX0" TYPE="LVM2_member" PARTUUID="13ba9979-05"

```

# La commande confirme que la partition sda5 est bien membre d'un groupe LVM, mais aussi qu'elle n'est pas **chiffrée** (sinon, le TYPE serait crypto\_LUKS). Sur une machine sensible, il est très important de chiffrer les partitions afin de rendre illisible leur contenu, ce qui s'avère utile en cas de vol par exemple.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier le chiffrement des partitions sensibles du système

# Ensuite, tout le système (sauf le noyau) tient dans une seule partition. Or, le partitionnement doit permettre d'isoler les composants du système de fichiers. De cette façon, il n'est pas possible, pour une application quelconque, de saturer de fichiers la partition système et de provoquer une interruption du service.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que le partitionnement isole et protège les composants du système (/boot ; /tmp ; /home ; /var ; /var/log ; )

Option	Description
async/sync	Les entrées/sorties sont asynchrones/synchrones
noauto/auto	Peut être montée automatiquement ou non
dev/nodev	Supporte ou non les fichiers de type périphérique
exec/noexec	Permet l'exécution ou non de fichier
suid/nosuid	Compatible avec le bit S-[U/G]ID
ro/rw	Lecture seule ou lecture/écriture
user/nouser	Peut être montée par un utilisateur privilégié ou non



```
bigboss@vm-audit:~$ mount | grep /dev/mapper
/dev/mapper/vm--audit--vg-root on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
```

# Si nous devons reprendre le partitionnement idéal évoqué ci-dessus, les options de montage recommandées seraient différentes pour chaque répertoire :

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier les options de montage suivants pour les répertoires /tmp ( rw, nosuid, nodev, noexec ) /home ( rw, nosuid, nodev, noexec ) /var ( rw, nosuid, nodev, noexec, sync ) /var/log ( rw, nosuid, nodev, noexec, sync )

```
bigboss@vm-audit:~$ ls -lrtha /boot/
total 49M
-rw----- 1 root root 6,8M juil. 18 2017 vmlinuz-4.4.0-87-generic
-rw----- 1 root root 3,8M juil. 18 2017 System.map-4.4.0-87-generic
-rw-r--r-- 1 root root 186K juil. 18 2017 config-4.4.0-87-generic
-rw-r--r-- 1 root root 1,2M juil. 18 2017 abi-4.4.0-87-generic
drwx----- 2 root root 12K juil. 3 2018 lost+found
drwxr-xr-x 23 root root 4,0K juil. 3 2018 ..
drwxr-xr-x 5 root root 1,0K juil. 3 2018 grub
-rw-r--r-- 1 root root 37M juil. 3 2018 initrd.img-4.4.0-87-generic
drwxr-xr-x 4 root root 1,0K juil. 3 2018 .
bigboss@vm-audit:~$
```

# **/boot** est une partition très sensible, car elle contient le noyau de Linux et la configuration dynamique de Grub. Le fichier **System.map** contient notamment la table des symboles utilisée par le noyau, c'est-à-dire la liste des variables et des fonctions associées à leurs adresses mémoire respectives. Bref, les pages jaunes du noyau en quelque sorte. Ce fichier est souvent la cible d'attaques visant à exploiter les failles dans le code du noyau.

Pour toutes ces raisons, la partition **/boot** doit bénéficier d'une attention particulière. Dans le meilleur des cas, il faut attribuer l'option **noauto** afin qu'elle ne soit pas montée automatiquement. Cependant, dans le cas où cette partition s'avérerait inévitable (par exemple pour changer de noyau), il faudrait alors la monter avec les options **ro**, **nosuid**, **nodev**, **noexec**, et la passer à **rw** pour l'utilisateur **root** uniquement lorsque nécessaire.

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifier la protection de la partition /boot

c) Les comptes utilisateurs, les mots de passes, les droits spéciaux et les mises à jours de sécurité

```
bigboss:$6$6WLo9XF$r$X/cvptAvd7iHJNy6Ig8jz79nPBKFUaCIkX0mvsYlHc7QJt9oIj1YiPRLPYTryZe7k10QzCfDC
NcrfvRn2kuF41:17715:0:99999:7:::
pierre:$6$/HJzmsr$iQqHcr/w0/Ye/nRcYHh0GjW9yamu21aho0LD03cfzosE6xamfyp6n3r5V9zY6M6oNcyBQHGt.e
kDeRjkk2oYx0:17716:0:99999:7:::
marie:$6$E19t3cN1$8iYBPvvEMA3LR4qKdIdEKExppisd0H9sgfe9bKTK1wcFAq7AuqLKZT.mGiKZYVY/qufoY2p/MQ
CY26iEZ/zH0:17716:0:99999:7:::
daniel:$6$uQ.s/U1V$SxPmVWC/4yjjaxxhd1pqxkvsPo30dddcTkWWTyPjNL4C1hdfIy1b1CdtugZ3dsoNkTOATFMVPM
```

# Historiquement, le fichier **/etc/passwd** contenait la liste des utilisateurs ET leurs mots de passe. Or ce fichier est accessible à tout le monde en lecture seule, ce qui permet à un attaquant d'en faire une copie et de déchiffrer les mots de passe. Désormais, Linux utilise le principe de mots de passe dits « **shadow** ». Ces mots de passe figurent dans un fichier **/etc/shadow**, lisible uniquement par root et chiffré.

```
bigboss@vm-audit: /etc/pam.d
bigboss@vm-audit:/etc/pam.d$ grep pam_pwquality /etc/pam.d/*
bigboss@vm-audit:/etc/pam.d$
```

# Le module **PAM** garantit aussi un minimum de **robustesse** des mots de passe. La librairie qui vérifie la robustesse des mots de passe est **pam\_pwquality.so** cependant ce module n'est pas installé.

Configuration	Description	Valeur par défaut
difok	Nombre de caractères dans le nouveau mot de passe, qui ne doivent pas être présents dans l'ancien	5
minlen	Longueur minimale	9 (>6 obligatoire)
ucredit	Nombre de majuscules	1
lcredit	Nombre de minuscules	1
dcredit	Nombre de chiffres	1
ocredit	Nombre de caractère non alphanumériques	1
maxrepeat	Nombre maximal de caractères se répétant	0 (désactivé)

### RECOMMANDATION-WARNING (défense en profondeur) : Vérifier la robustesse des mots de passe en installant et configurant le module **pam\_pwquality**

Si dans le fichier des utilisateurs du système ( /etc/passwd) le champ indique **/sbin/nologin**, alors le *shell* exécuté renverra simplement un message d'erreur à l'utilisateur. Ainsi, il est déjà possible de filtrer les comptes qui peuvent se connecter.

```
bigboss@vm-audit: /etc/pam.d
bigboss@vm-audit:/etc/pam.d$ cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:/:/home/syslog:/bin/false
_apt:x:105:65534:/:/nonexistent:/bin/false
lxd:x:106:65534:/:/var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112:/:/var/run/dbus:/bin/false
uidd:x:109:113:/:/run/uidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
bind:x:111:116:/:/var/cache/bind:/bin/false
postfix:x:112:118:/:/var/spool/postfix:/bin/false
dovecot:x:113:120:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovecotnull:x:114:121:Dovecot login user,,,:/nonexistent:/bin/false
bigboss:x:1000:1000:bigboss,,,:/home/bigboss:/bin/bash
pierre:x:1001:1001:Pierre,,,:/home/pierre:/bin/bash
marie:x:1002:1002:Marie,,,:/home/marie:/bin/bash
daniel:x:1001:1001:Daniel,,,:/home/daniel:/bin/bash
```

```
bigboss@vm-audit:/$ sudo chage -l marie
Last password change           : juil. 04, 2018
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
bigboss@vm-audit:/$ sudo chage -l pierre
Last password change           : juil. 04, 2018
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
bigboss@vm-audit:/$ sudo chage -l bigboss
Last password change           : juil. 03, 2018
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
bigboss@vm-audit:/$ sudo chage -l root
Last password change           : juil. 03, 2018
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
bigboss@vm-audit:/$ sudo chage -l daniel
chage: user 'daniel' does not exist in /etc/passwd
```

# Nous obtenons également ici un exemple typique de configuration par défaut, où l'utilisateur n'est pas forcé de changer son mot de passe.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que les comptes utilisateurs qui peuvent se connecter ont pour obligation de changer leur mot de passe régulièrement

**RECOMMANDATION-WARNING** (défense en profondeur) : Vérifier les valeurs par défaut des attributs des mots de passe pour chaque compte utilisateur dans **/etc/login.defs**

# Nous pouvons également voir que l'utilisateur "daniel" n'existe pas or ce dernier avait la possibilité de se connecter avec un shell car il n'est pas en nologin. Daniel a le même UID que Pierre. Plusieurs questions, qui est Daniel ? Son répertoire est vide mais est-ce ce qu'il a supprimé son compte après une potentiel intrusion malveillante ?

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que l'utilisateur Daniel existe pour l'entreprise sinon prendre les mesures pour s'informer des derniers événements de l'utilisateur et supprimer définitivement son accès.

# Il est également primordiale d'avoir une liste de fichier connu et maîtriser disposant des droits **setuid** ( perm = 4000 ), **setgid** ( perm = 6000 ), **sticky bit** ( perm = 1000 ). En effet il faut absolument éviter qu'une commande n'utilise sont élévation de privilège temporaire dans un périmètre d'action plus ou moins large de n'importe que façon.

```
bigboss@vm-audit:/$ find / -type f -perm /4000 -ls 2>/dev/null
20020      40 -rwsr-xr-x  1 root    root      38984 juin 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
21041     420 -rwsr-xr-x  1 root    root     428240 mars 16  2017 /usr/lib/openssh/ssh-keysign
22428     204 -rwsr-xr-x  1 root    root     208680 avril 29  2017 /usr/lib/snapd/snap-confine
22290      16 -rwsr-xr-x  1 root    root     14864 janv. 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
   590     12 -rwsr-xr-x  1 root    root     10232 mars 27  2017 /usr/lib/eject/dmccrypt-get-device
18117     44 -rwsr-xr--  1 root    messagebus 42992 janv. 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   405     56 -rwsr-xr-x  1 root    root     54256 mai 17  2017 /usr/bin/passwd
22298     24 -rwsr-xr-x  1 root    root     23376 janv. 18  2016 /usr/bin/pkexec
20055     36 -rwsr-xr-x  1 root    root     32944 mai 17  2017 /usr/bin/newuidmap
   394     40 -rwsr-xr-x  1 root    root     39904 mai 17  2017 /usr/bin/newgrp
   269     40 -rwsr-xr-x  1 root    root     40432 mai 17  2017 /usr/bin/chsh
   330     76 -rwsr-xr-x  1 root    root     75304 mai 17  2017 /usr/bin/gpasswd
20056     36 -rwsr-xr-x  1 root    root     32944 mai 17  2017 /usr/bin/newgidmap
   489    136 -rwsr-xr-x  1 root    root    136808 juil.  4  2017 /usr/bin/sudo
22301     88 -rwsr-sr-x  1 root    mail      89248 mai 15  2015 /usr/bin/procmail
   267     52 -rwsr-xr-x  1 root    root     49584 mai 17  2017 /usr/bin/chfn
21387     52 -rwsr-sr-x  1 daemon  daemon    51464 janv. 14  2016 /usr/bin/at
260207    28 -rwsr-xr-x  1 root    root     27608 juin 14  2017 /bin/umount
273185   140 -rwsr-xr-x  1 root    root    142032 janv. 28  2017 /bin/ntfs-3g
260172    44 -rwsr-xr-x  1 root    root     44168 mai  7  2014 /bin/ping
260158    40 -rwsr-xr-x  1 root    root     40152 juin 14  2017 /bin/mount
260173    44 -rwsr-xr-x  1 root    root     44680 mai  7  2014 /bin/ping6
260189    40 -rwsr-xr-x  1 root    root     40128 mai 17  2017 /bin/su
273647    32 -rwsr-xr-x  1 root    root     30800 juil. 12  2016 /bin/fusermount
```

```
bigboss@vm-audit:/$ find / -type f -perm /6000 -ls 2>/dev/null
20020      40 -rwsr-xr-x  1 root    root      38984 juin 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
21571     12 -rwxr-sr-x  1 root    utmp      10232 mars 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
21041     420 -rwsr-xr-x  1 root    root     428240 mars 16  2017 /usr/lib/openssh/ssh-keysign
22428     204 -rwsr-xr-x  1 root    root     208680 avril 29  2017 /usr/lib/snapd/snap-confine
22290      16 -rwsr-xr-x  1 root    root     14864 janv. 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
   590     12 -rwsr-xr-x  1 root    root     10232 mars 27  2017 /usr/lib/eject/dmccrypt-get-device
18117     44 -rwsr-xr--  1 root    messagebus 42992 janv. 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
21450     20 -r-xr-sr-x  1 root    postdrop  18376 avril 13  2016 /usr/sbin/postqueue
21462     16 -r-xr-sr-x  1 root    postdrop  14328 avril 13  2016 /usr/sbin/postdrop
   405     56 -rwsr-xr-x  1 root    root     54256 mai 17  2017 /usr/bin/passwd
21061     352 -rwxr-sr-x  1 root    ssh       358624 mars 16  2017 /usr/bin/ssh-agent
   315     24 -rwxr-sr-x  1 root    shadow    22768 mai 17  2017 /usr/bin/expiry
22231     12 -rwxr-sr-x  1 root    mail      10664 févr. 17  2016 /usr/bin/mutt_dotlock
18337     16 -rwxr-sr-x  1 root    tty       14752 mars  1  2016 /usr/bin/bsd-write
   278     36 -rwxr-sr-x  1 root    crontab   36080 avril  5  2016 /usr/bin/crontab
22298     24 -rwsr-xr-x  1 root    root     23376 janv. 18  2016 /usr/bin/pkexec
19962     16 -rwxr-sr-x  1 root    mail      14856 déc.  7  2013 /usr/bin/dotlockfile
   264     64 -rwxr-sr-x  1 root    shadow    62336 mai 17  2017 /usr/bin/chage
20055     36 -rwsr-xr-x  1 root    root     32944 mai 17  2017 /usr/bin/newuidmap
   394     40 -rwsr-xr-x  1 root    root     39904 mai 17  2017 /usr/bin/newgrp
   269     40 -rwsr-xr-x  1 root    root     40432 mai 17  2017 /usr/bin/chsh
   330     76 -rwsr-xr-x  1 root    root     75304 mai 17  2017 /usr/bin/gpasswd
22302     20 -rwxr-sr-x  1 root    mail      18704 mai 15  2015 /usr/bin/lockfile
20056     36 -rwsr-xr-x  1 root    root     32944 mai 17  2017 /usr/bin/newgidmap
   489    136 -rwsr-xr-x  1 root    root    136808 juil.  4  2017 /usr/bin/sudo
22301     88 -rwsr-sr-x  1 root    mail      89248 mai 15  2015 /usr/bin/procmail
21577     428 -rwxr-sr-x  1 root    utmp      434216 févr.  7  2016 /usr/bin/screen
   542     28 -rwxr-sr-x  1 root    tty       27368 juin 14  2017 /usr/bin/wall
20981     40 -rwxr-sr-x  1 root    mlocate   39520 nov. 18  2014 /usr/bin/mlocate
   267     52 -rwsr-xr-x  1 root    root     49584 mai 17  2017 /usr/bin/chfn
21387     52 -rwsr-sr-x  1 daemon  daemon    51464 janv. 14  2016 /usr/bin/at
   194     36 -rwxr-sr-x  1 root    shadow    35632 mars 16  2016 /sbin/pam_extrausers_chkpwd
   230     36 -rwxr-sr-x  1 root    shadow    35600 mars 16  2016 /sbin/unix_chkpwd
260207    28 -rwsr-xr-x  1 root    root     27608 juin 14  2017 /bin/umount
273185   140 -rwsr-xr-x  1 root    root    142032 janv. 28  2017 /bin/ntfs-3g
260172    44 -rwsr-xr-x  1 root    root     44168 mai  7  2014 /bin/ping
260158    40 -rwsr-xr-x  1 root    root     40152 juin 14  2017 /bin/mount
260173    44 -rwsr-xr-x  1 root    root     44680 mai  7  2014 /bin/ping6
260189    40 -rwsr-xr-x  1 root    root     40128 mai 17  2017 /bin/su
273647    32 -rwsr-xr-x  1 root    root     30800 juil. 12  2016 /bin/fusermount
```

```
bigboss@vm-audit:/$ sudo find / -type d -perm -1000 -exec ls -ld {} \;
[sudo] Mot de passe de bigboss :
drwxrwxrwt 5 root root 120 juil. 26 21:12 /run/lock
drwx-wx-wt 2 root root 4096 juil. 14 13:09 /var/lib/php/sessions
drwxrwxrwt 6 root root 4096 juil. 26 21:12 /var/tmp
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /var/tmp/systemd-private-4085196392e9465d8d3976b90ece4ccd-systemd-timesyncd.service-f14Tio/tmp
drwxrwxrwt 2 root root 4096 juil.  3 2018 /var/tmp/systemd-private-16aa0867554b43e5b96a6f6175b0973f-dovecot.service-NTjERn/tmp
drwxrwxrwt 2 root root 4096 juil.  3 2018 /var/tmp/systemd-private-16aa0867554b43e5b96a6f6175b0973f-systemd-timesyncd.service-Hsa2go/tmp
drwxrwx--T 2 daemon daemon 4096 juil.  3 2018 /var/spool/cron/atjobs
drwxrwx--T 2 daemon daemon 4096 janv. 14 2016 /var/spool/cron/atpool
drwx-wx--T 2 root crontab 4096 avril  5 2016 /var/spool/cron/crontabs
drwx-wx--T 2 postfix postdrop 4096 juil.  4 2018 /var/spool/postfix/maildrop
drwxrwxrwt 2 root root 4096 juil.  3 2018 /var/crash
drwxrwxrwt 2 root root 40 juil. 26 21:12 /dev/mqueue
drwxrwxrwt 2 root root 40 juil. 26 21:12 /dev/shm
drwxrwxrwt 9 root root 4096 juil. 27 03:39 /tmp
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/.X11-unix
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/.Test-unix
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/.XIM-unix
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/.font-unix
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/systemd-private-4085196392e9465d8d3976b90ece4ccd-dovecot.service-hWp1C8/tmp
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/.ICE-unix
drwxrwxrwt 2 root root 4096 juil. 26 21:12 /tmp/systemd-private-4085196392e9465d8d3976b90ece4ccd-systemd-timesyncd.service-L41nBL/tmp
```

**RECOMMANDATION-CRITICAL** (moindre privilège) : Examiner et maîtriser la liste des fichiers avec les droits spéciaux setuid, setgid et sticky bit

# Il est aussi nécessaire de créer un groupe d'utilisateur identifiés comme administrateur afin de limiter l'élévation de privilège de **la commande sudo**

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifier la présence d'un groupe d'utilisateurs identifié comme administrateur de la machine et disposant des droits de changement de privilèges par l'intermédiaire d'un processus type sudo

```
bigboss@vm-audit: /
bigboss@vm-audit:/$ ls -lrtha /usr/bin/sudo
-rwsr-xr-x 1 root root 134K juil.  4 2017 /usr/bin/sudo
```

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifier que la commande **sudo** peut être exécutée uniquement par le groupe administrateur (+ root)

# Ensuite, il est nécessaire de vérifier que le groupe admin dispose bien au minimum des droits pour exécuter les commandes nécessaires au maintien du système dans le fichier **/etc/sudoers**. Au mieux, toutes les commandes possibles.

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifier que le fichier de configuration **/etc/sudoers** contient la déclaration des commandes nécessaires au maintien du système pour les utilisateurs du groupe administrateur

#### d) La configuration des services lancés

```
bigboss@vm-audit: ~
bigboss@vm-audit:~$ systemctl list-unit-files --type service --state enabled
UNIT FILE                                STATE
accounts-daemon.service                 enabled
atd.service                             enabled
autovt@.service                         enabled
bind9.service                           enabled
cron.service                            enabled
dovecot.service                         enabled
fail2ban.service                        enabled
friendly-recovery.service               enabled
getty@.service                          enabled
iscsi.service                           enabled
iscsid.service                          enabled
lvm2-monitor.service                   enabled
lxcfs.service                           enabled
lxd-containers.service                  enabled
mysql.service                           enabled
networking.service                     enabled
open-iscsi.service                      enabled
open-vm-tools.service                   enabled
resolvconf.service                      enabled
rsyslog.service                         enabled
snapd.autoimport.service                enabled
snapd.service                           enabled
snapd.system-shutdown.service           enabled
ssh.service                             enabled
sshd.service                            enabled
syslog.service                          enabled
systemd-timesyncd.service                enabled
ufw.service                             enabled
unattended-upgrades.service              enabled
ureadahead.service                      enabled
```

# Afin d'augmenter la sécurité nécessaire face aux différentes fonctionnalités que chaque service actif propose, il est recommandé de :

Ne pas afficher la bannière du service, qui renvoie par défaut les informations sur la version du service et son système d'exploitation. Une simple commande telnet ou netcat permet de récupérer ces informations très utiles pour un attaquant

Pour chaque répertoire, la présence de la directive **Options -Indexes**, qui permet d'empêcher de lister le contenu du répertoire.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier et appliquer le durcissement de la configuration des services lancés

### e) Le cloisonnement des services lancés

```
bigboss@vm-audit:~$ ps -edf | grep accounts-daemon
root      853      1  0 05:16 ?        00:00:00 /usr/lib/accountsservice/account
s-daemon
bigboss   1631   1611  0 05:54 pts/0    00:00:00 grep --color=auto accounts-daemo
n
bigboss@vm-audit:~$ ps -edf | grep atd
daemon    859      1  0 05:16 ?        00:00:00 /usr/sbin/atd -f
bigboss   1633   1611  0 05:54 pts/0    00:00:00 grep --color=auto atd
bigboss@vm-audit:~$ ps -edf | grep autovt
bigboss   1635   1611  0 05:54 pts/0    00:00:00 grep --color=auto autovt
bigboss@vm-audit:~$ ps -edf | grep bind9
bigboss   1637   1611  0 05:54 pts/0    00:00:00 grep --color=auto bind9
bigboss@vm-audit:~$ ps -edf | grep cron
root      865      1  0 05:16 ?        00:00:00 /usr/sbin/cron -f
bigboss   1639   1611  0 05:55 pts/0    00:00:00 grep --color=auto cron
bigboss@vm-audit:~$ ps -edf | grep dovecot
root      1136     1  0 05:16 ?        00:00:00 /usr/sbin/dovecot
dovecot   1149   1136  0 05:16 ?        00:00:00 dovecot/anvil
root      1150   1136  0 05:16 ?        00:00:00 dovecot/log
root      1182   1136  0 05:16 ?        00:00:00 dovecot/config
bigboss   1641   1611  0 05:55 pts/0    00:00:00 grep --color=auto dovecot
bigboss@vm-audit:~$ ps -edf | grep fail2ban
root      1257     1  0 05:16 ?        00:00:00 /usr/bin/python3 /usr/bin/fail2b
an-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -
x -b
bigboss   1644   1611  0 05:55 pts/0    00:00:00 grep --color=auto fail2ban
bigboss@vm-audit:~$ ps -edf | grep friendly-recovery
bigboss   1646   1611  0 05:55 pts/0    00:00:00 grep --color=auto friendly-recov
ery
```

```
bigboss@vm-audit:~$ ps -edf | grep getty
bigboss   1648   1611  0 05:55 pts/0    00:00:00 grep --color=auto getty
bigboss@vm-audit:~$ ps -edf | grep iscsi
root      406      2  0 05:16 ?        00:00:00 [iscsi_eh]
root      1122     1  0 05:16 ?        00:00:00 /sbin/iscsid
root      1123     1  0 05:16 ?        00:00:00 /sbin/iscsid
bigboss   1650   1611  0 05:56 pts/0    00:00:00 grep --color=auto iscsi
bigboss@vm-audit:~$ ps -edf | grep lvm2-monitor
bigboss   1652   1611  0 05:56 pts/0    00:00:00 grep --color=auto lvm2-monitor
bigboss@vm-audit:~$ ps -edf | grep lxcfs
root      884      1  0 05:16 ?        00:00:00 /usr/bin/lxcfs /var/lib/lxcfs/
bigboss   1654   1611  0 05:56 pts/0    00:00:00 grep --color=auto lxcfs
bigboss@vm-audit:~$ ps -edf | grep lxd-containers
bigboss   1656   1611  0 05:56 pts/0    00:00:00 grep --color=auto lxd-container
bigboss@vm-audit:~$ ps -edf | grep mysql
mysql     1132     1  0 05:16 ?        00:00:00 /usr/sbin/mysqld
bigboss   1658   1611  0 05:56 pts/0    00:00:00 grep --color=auto mysql
bigboss@vm-audit:~$ ps -edf | grep networking
bigboss   1660   1611  0 05:57 pts/0    00:00:00 grep --color=auto networking
bigboss@vm-audit:~$ ps -edf | grep rsyslog
syslog    851      1  0 05:16 ?        00:00:00 /usr/sbin/rsyslogd -n
bigboss   1662   1611  0 05:57 pts/0    00:00:00 grep --color=auto rsyslog
bigboss@vm-audit:~$ ps -edf | grep ssh
root      1089     1  0 05:16 ?        00:00:00 /usr/sbin/sshd -D
root      1579   1089  0 05:52 ?        00:00:00 sshd: bigboss [priv]
bigboss   1610   1579  0 05:52 ?        00:00:00 sshd: bigboss@pts/0
bigboss   1664   1611  0 05:57 pts/0    00:00:00 grep --color=auto ssh
bigboss@vm-audit:~$ ps -edf | grep sshd
root      1089     1  0 05:16 ?        00:00:00 /usr/sbin/sshd -D
root      1579   1089  0 05:52 ?        00:00:00 sshd: bigboss [priv]
bigboss   1610   1579  0 05:52 ?        00:00:00 sshd: bigboss@pts/0
bigboss   1666   1611  0 05:57 pts/0    00:00:00 grep --color=auto sshd
bigboss@vm-audit:~$ ps -edf | grep syslog
syslog    851      1  0 05:16 ?        00:00:00 /usr/sbin/rsyslogd -n
root      918      1  0 05:16 ?        00:00:00 /sbin/mdadm --monitor --pid-file
/run/mdadm/monitor.pid --daemonise --scan --syslog
bigboss   1668   1611  0 05:58 pts/0    00:00:00 grep --color=auto syslog
bigboss@vm-audit:~$ ps -edf | grep snapd
root      855      1  0 05:16 ?        00:00:00 /usr/lib/snapd/snapd
bigboss   1670   1611  0 05:58 pts/0    00:00:00 grep --color=auto snapd
bigboss@vm-audit:~$ ps -edf | grep httpd
```

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifier les comptes système associés aux services

```
bigboss@vm-audit: ~  
bigboss@vm-audit:~$ ls -lrtha /var/www/  
total 12K  
drwxr-xr-x  3 root root 4,0K juil.  3 2018 .  
drwxr-xr-x 14 root root 4,0K juil.  3 2018 ..  
drwxr-xr-x  3 root root 4,0K juil.  4 2018 html  
bigboss@vm-audit:~$
```

# Ici, le répertoire est la propriété du compte root et tout le monde peut y accéder. Cette configuration par défaut n'est donc pas acceptable pour un serveur web.

**RECOMMANDATION-CRITICAL** (moindre privilège) : Vérifiez les droits du système de fichiers associé aux comptes système exécutant des services

# Dans l'idéal, il faudrait attribuer une machine et un système d'exploitation à chaque service. Cette solution drastique est coûteuse en matériel et en maintenance. Aujourd'hui, il existe plusieurs solutions d'isolation moins coûteuses :

Les conteneurs, où un même noyau gère plusieurs instances système

La virtualisation, où un hyperviseur gère plusieurs machines virtuelles émulées sur la même machine physique

Un hyperviseur noyau, comme Linux KVM.

**RECOMMANDATION-WARNING** (défense en profondeur) : Vérifier qu'il est possible de virtualiser l'architecture applicative du serveur

# Il est également possible d'isoler directement un processus ainsi que les utilisateurs s'y connectant. Il est possible pour cela d'utiliser respectivement la commande **chroot** ou le module **pam\_chroot.so**

Cependant, le processus d'isolation chroot présente quelques faiblesses :

Le cloisonnement est limité en ce qui concerne les accès aux systèmes de fichiers, mais pas en ce qui concerne les accès aux processus ou aux réseaux ;

Les utilisateurs peuvent sortir de leur environnement spécifique en utilisant des processus externes.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que le chrootage est utilisé sur les services lancés dans la mesure du possible

## f) Les fichiers de trace des services

```
bigboss@vm-audit:~$ ls -lrtha /var/log/
total 1,7M
drwxr-xr-x  2 root  root  4,0K juin  8  2017 lxd
drwxr-xr-x  2 root  root  4,0K juil. 19  2017 dist-upgrade
-rw-r----- 1 root  adm   31 août  1  2017 dmesg
-rw-r--r--  1 root  root   57K août  1  2017 bootstrap.log
drwxr-xr-x  2 root  root  4,0K juil.  3  2018 fsck
drwxr-xr-x  2 root  root  4,0K juil.  3  2018 apt
drwxr-x---  2 root  adm   4,0K juil.  3  2018 apache2
drwxr-x---  2 mysql  adm   4,0K juil.  3  2018 mysql
drwxr-xr-x 14 root  root  4,0K juil.  3  2018 ..
drwxr-xr-x  3 root  root  4,0K juil.  3  2018 installer
-rw-r--r--  1 root  root   32K juil.  4  2018 faillog
drwxr-xr-x  2 root  root  4,0K juil.  4  2018 dbconfig-common
-rw-r--r--  1 root  root   26K juil.  4  2018 alternatives.log
drwxrwxr-x 11 root  syslog 4,0K juil.  4  2018 .
-rw-r--r--  1 root  root  521K juil.  4  2018 dpkg.log
drwxr-x---  2 root  adm   4,0K juil. 14 13:09 unattended-upgrades
-rw-----  1 root  utmp   1,9K juil. 21 16:00 btmp
-rw-r----- 1 root  adm   9,4K juil. 27 05:16 fail2ban.log
-rw-r----- 1 syslog adm  293K juil. 27 05:16 kern.log
-rw-r----- 1 syslog adm   18K juil. 27 05:16 mail.log
-rw-rw-r--  1 root  utmp   17K juil. 27 05:52 wtmp
-rw-rw-r--  1 root  utmp  287K juil. 27 05:52 lastlog
-rw-r----- 1 syslog adm   35K juil. 27 06:09 auth.log
-rw-r----- 1 syslog adm  549K juil. 27 06:10 syslog
bigboss@vm-audit:~$
```

Chacun de ces fichiers joue un rôle important dans la supervision du système d'exploitation. Ils doivent donc être présents et modifiables uniquement par **root, mysql ou syslog**

# Cloisonner le service Syslog par plusieurs opérations distinctes :

Privilégier une partition spécifique pour les fichiers de trace, afin de vous assurer qu'un processus tiers ne viendra pas saturer la partition des fichiers de trace ;

Instaurer un processus de rotation des fichiers de trace en les compressant. Les fichiers de trace sont souvent volumineux et la création de nouveaux fichiers de manière régulière permet une maintenance plus simple des archives. Cette configuration est stockée dans le fichier `/etc/logrotate.conf` :

Externaliser et centraliser les fichiers de trace. Dans la mesure du possible, écrivez les traces dans les fichiers de l'arborescence locale, mais aussi dans des fichiers distants, en passant par le service réseau d'un serveur de centralisation des logs. Pour cela, il suffit d'indiquer, dans le fichier de configuration `/etc/rsyslog.conf`, la destination réseau du fichier distant (via UDP ou TCP)

### **RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier le cloisonnement du service Syslog

Il est important de mettre en place un service cloisonné et sécurisé de gestion des traces. Cependant, les événements critiques, les tentatives de connexion échouées, les requêtes vers des ressources Web inexistantes figureront toujours dans les fichiers de trace. Il est primordial de superviser ces fichiers car, si vous ne les lisez pas, vous ne saurez pas ce qu'il se passe sur le serveur.

Il existe plusieurs façons de connaître le contenu de ces fichiers :



Dégager du temps pour **consulter manuellement** le contenu des fichiers pour vérifier les élévations de privilèges, échecs de connexions et autres problèmes directement liés au système via syslog. C'est la technique la plus simple, mais la plus coûteuse en termes de temps ;

Installer un **processus de supervision automatique** du contenu des fichiers. Par exemple des sondes **Nagios** qui viendraient consulter, à intervalle de temps régulier, les lignes des fichiers, afin de lever des alertes lorsque nécessaire ;

Installer un **parseur de fichiers de trace**. Celui-ci permet notamment de recevoir, par mail, un résumé des lignes jugées critiques dans tous les fichiers parsés. **Logwatch** est très efficace en la matière

**RECOMMANDATION-WARNING** (défense en profondeur) : Mettre en place le processus de supervision des fichiers de trace

## 5 - Auditer les accès réseaux

### a) Les ports ouverts du serveur et les processus associés

```
bigboss@vm-audit:~$ ss -lptun
Netid State Recv-Q Send-Q Local Address:Port
udp UNCONN 0 0 192.168.43.246:53
udp UNCONN 0 0 127.0.0.1:53
udp UNCONN 0 0 *:68
udp UNCONN 0 0 :::53
tcp LISTEN 0 100 *:110
tcp LISTEN 0 100 *:143
tcp LISTEN 0 10 192.168.43.246:53
tcp LISTEN 0 10 127.0.0.1:53
tcp LISTEN 0 128 *:22
tcp LISTEN 0 100 *:25
tcp LISTEN 0 128 127.0.0.1:953
tcp LISTEN 0 80 :::3306
tcp LISTEN 0 100 :::110
tcp LISTEN 0 100 :::143
tcp LISTEN 0 128 :::80
tcp LISTEN 0 10 :::53
tcp LISTEN 0 128 :::22
tcp LISTEN 0 100 :::25
tcp LISTEN 0 128 :::1953
bigboss@vm-audit:~$ netstat -laptun | grep LISTEN
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir toutes.)
tcp 0 0 0.0.0.0:110 0.0.0.0:* LISTEN 0 15739 -
tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN 0 15751 -
tcp 0 0 192.168.43.246:53 0.0.0.0:* LISTEN 111 16928 -
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN 111 16821 -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 0 15449 -
tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 0 17464 -
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN 111 16963 -
tcp6 0 0 :::3306 :::* LISTEN 107 17074 -
tcp6 0 0 :::110 :::* LISTEN 0 15740 -
tcp6 0 0 :::143 :::* LISTEN 0 15752 -
tcp6 0 0 :::80 :::* LISTEN 0 17000 -
tcp6 0 0 :::53 :::* LISTEN 111 16817 -
tcp6 0 0 :::22 :::* LISTEN 0 15451 -
tcp6 0 0 :::25 :::* LISTEN 0 17465 -
tcp6 0 0 :::1953 :::* LISTEN 111 16966 -
bigboss@vm-audit:~$
```

D'après les informations ci dessus, certaines configurations réseaux ne sont pas indispensables au serveur afin d'optimiser la sécurité réseau.

# Privilégier un adressage réseau manuel et non automatique en désactivant le service DHCP ( port 68 ). Si un appareil non autorisé devait se connecter

directement sur le serveur, ce dernier ne recevra aucun accès au LAN de l'entreprise. La seule possibilité serait de connaître pour l'attaquant le plan d'adressage. Toutefois, pour contrer cette dernière possibilité, une méthode d'affinage des besoins en adresse IP permettra de limiter le masque de sous réseau aux besoin exact afin de ne pas adresser manuellement une IP supplémentaire.

**RECOMMANDATION-CRITICAL** (minimisation) : Désactiver le service DHCP et adresser le réseau manuellement pour le serveur. Dans la mesure du possible, réduire le masque de sous réseau aux besoins exact d'adresse IP. ( Prendre en compte la scalabilité de l'entreprise si croissance rapide )

Si le serveur n'utilise pas un service de messagerie pour automatisation de mail, ou autre alors **les ports 110 ( POP3 ) & IMAP ( 143 )** ne sont pas nécessaire mais conseillé. En effet, comme nous avons pu voir précédemment, il est important de mettre en place un système de supervision de logs avec nagios par exemple. **La remonté des alertes se faisant automatiquement par mail, ce type de service de messagerie sera alors vitale et apportera davantage de valeur ajouté que de contrainte liée à la sécurité**, en veillant toutefois à garder le service de messagerie à jour.

Puisque le serveur est un serveur web, il est primordiale de garder également les ports des services **SSH, FTP, HTTP/HTTPS, DNS**, respectivement **22, 25, 80/443, 53 ouverts**. Le protocole TCP/IP & UDP/IP nécessite également l'ouverture du port 953 afin que le serveur puisse envoyer des trames réseaux.

```
bigboss@vm-audit:~$ ss -lptun
tcp LISTEN 0 80 :::3306
```

# Cette ligne indique que le service est en écoute sur sur le port 3306. Cette configuration ne convient pas, car il est très peu probable qu'il soit possible d'accéder au service de base de données directement depuis l'environnement externe du serveur. Nous pouvons même dire qu'une connexion interne en provenance des codes sources de l'application sera largement suffisante.

**RECOMMANDATION-CRITICAL** (minimisation) : Désactiver le port 3306 en écoute depuis l'extérieur pour le service de base de donnée.

# Par ailleurs, et dans la mesure du possible, si les services associés ne sont pas publics, il est fortement recommandé de changer les ports d'accès par défaut à ces services, car ce sont des cibles pour les attaquants.

**RECOMMANDATION-WARNING** (défense en profondeur) : Vérifier que les ports par défaut des services ont été changés dans la mesure du possible

b) Les processus de filtrage réseau, pare feu et proxy

Le **filtrage réseau** consiste à analyser le trafic entrant et sortant du serveur, et à établir des règles définissant les actions à effectuer sur ce trafic. Cette fonctionnalité est exécutée directement par le noyau Linux.

Le premier processus de filtrage réseau sous Linux est le **TCP Wrapper**. Cette technique s'appuie sur la librairie partagée **libwrap** et permet de définir des règles d'accès sur deux fichiers de configuration :

Le fichier **/etc/hosts.allow**, qui contient la liste des règles autorisant la connexion à un service ;

Le fichier **/etc/hosts.deny**, qui contient la liste des règles refusant la connexion à un service.

```
bigboss@vm-audit:/usr/sbin$ ldd sshd | grep libwrap
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007fc0a9b48000)
bigboss@vm-audit:/usr/sbin$ ldd mysqld | grep libwrap
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007fe607af5000)
bigboss@vm-audit:/usr/sbin$ ldd tcpd | grep libwrap
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007f6740eb8000)
bigboss@vm-audit:/usr/sbin$
```

# Les résultats montrent que les services **sshd**, **mysql**, **tcpd** sont compatibles avec la fonctionnalité **TCP Wrapper** pour ce serveur web.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier que les TCP Wrappers sont configurés pour les services réseau compatibles

```
bigboss@vm-audit:/usr/sbin$ grep IPTABLES /boot/config-`uname -r`
CONFIG_IP_NF_IPTABLES=m
CONFIG_IP6_NF_IPTABLES=m
bigboss@vm-audit:/usr/sbin$
```

Le second processus de filtrage réseau est le *firewall* **Netfilter**, codé directement dans le noyau Linux. Ce firewall fonctionne avec un système composé de trois principaux éléments : Chaînes, Règles & Actions

# La commande ci-dessus indique que le code Netfilter est compilé comme un module et qu'il est nécessaire de le charger pour accéder aux fonctionnalités du *firewall*. Cela ne convient pas au vu de la recommandation que nous avons émise sur le noyau (« Bloquer le chargement de modules supplémentaires »).

**RECOMMANDATION-WARNING** (minimisation) : Vérifier qu'il est possible d'accéder au *firewall* Netfilter par le noyau sans la contrainte module

```
bigboss@vm-audit:/usr/sbin$ sudo iptables -L -n
[sudo] Mot de passe de bigboss :
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
f2b-sshd   tcp  --  0.0.0.0/0              0.0.0.0/0          multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain f2b-sshd (1 references)
target     prot opt source                destination
RETURN    all  --  0.0.0.0/0              0.0.0.0/0
```

# Le résultat de cette commande affiche une configuration par défaut typique : une vraie passoire ! Le *firewall* dispose d'une seule règle et est configuré par défaut sur l'action **ACCEPT**. Évidemment, cette situation ne convient pas.

Il faudrait déjà passer la configuration par défaut en **DROP**.

Et ensuite laisser entrer uniquement les paquets ( **INPUT** ) à destination des services : HTTP/HTTPS, DNS, FTP, IMAP, POP3, SSH ( destination le réseau du plan d'adressage définit )

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier et appliquer que les règles Netfilter sont bien positionnées pour les configurations par défauts et les services du serveur web.

# Idéalement, il faudrait cloisonner par virtualisation, containers ou serveur physique chaque service web ( apache, mysql & le service applicatif ) avec également des masques de sous réseaux différents et par VLAN. Il faudrait également configurer le frontal web avec des règles iptables en **FORWARD** afin que chaque requête extérieur transite de façon sécurisé jusqu'au service requis du LAN, bloquant toutes les autres connexions indésirables entrantes pour le serveur de base de donnée et le serveur applicatif.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Dans la mesure du possible, cloisonner les services du serveur web et appliquer des règles FORWARD sur un plan d'adressage définit pour chaque service

Les **sysctl** du noyau sont des variables accessibles par l'administrateur et permettent d'influer sur le comportement du noyau pour certains aspects de son périmètre fonctionnel, comme les pages mémoires, les systèmes de fichiers ou encore le réseau.

# Il existe de nombreuses **sysctl** pour le réseau. Chacune permet de renforcer un peu plus la sécurité réseau de la machine. Nous allons ici recenser les plus communes et leur implication :

SYSCTL	Description
net.ipv4.ip_forward = 0	Absence de routage sur les interfaces
net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0	Refus des paquets de source <i>routing</i>
net.ipv4.icmp_echo_ignore_broadcasts = 1	Configuration contre les tempêtes ICMP ( <i>Smurf attacks</i> )
net.ipv4.accept_source_route = 0	Configuration contre les paquets contenant leur propre routage (utile seulement aux attaquants)
net.ipv4.rp_filter = 1	Configuration contre les paquets avec une IP incohérente avec l'interface réseau de destination ( <i>Spoofing</i> )

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Vérifier le positionnement des sysctl réseau communes au noyau dans le fichier **/etc/sysctl.conf**

### c) Les services SSH et FTP

# S'il y a une chose qu'il faut absolument bannir en ce qui concerne le service SSH, c'est la possibilité de se connecter directement avec le compte **root**. Ce réglage est indiqué dans le fichier de configuration avec la directive **PermitRootLogin**

```
bigboss@vm-audit: /
bigboss@vm-audit:/$ grep PermitRootLogin /etc/ssh/sshd_config
PermitRootLogin yes
# the setting of "PermitRootLogin without-password".
bigboss@vm-audit:/$ █
```

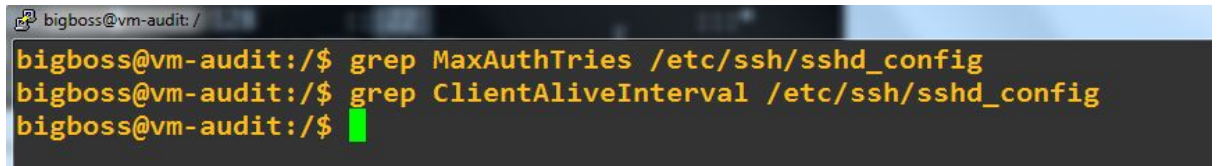
**RECOMMANDATION-CRITICAL** (moindre privilège) : Restreindre la directive PermitRootLogin du service SSH

# Par défaut, ssh écoute sur le port 22. Il faut changer ce port afin de compliquer le travail des attaquants !

```
bigboss@vm-audit: /
bigboss@vm-audit:/$ grep Port /etc/ssh/sshd_config
Port 22
bigboss@vm-audit:/$ █
```

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Changer le port d'écoute par défaut du service SSH

# Empêcher des sessions connectées sans activité (*idle*) & tracer les tentatives de connexion échouées en détail. Comme le montre la capture ci-dessous, aucune de ces configurations n'est appliqués pour le service SSH du serveur.



```
bigboss@vm-audit: /
bigboss@vm-audit:/$ grep MaxAuthTries /etc/ssh/sshd_config
bigboss@vm-audit:/$ grep ClientAliveInterval /etc/ssh/sshd_config
bigboss@vm-audit:/$ █
```

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Appliquer un blocage idle et tracer les tentatives de connexions échouées

# Enfin, dans le meilleur des cas, il est possible d'indiquer au service SSH de procéder à l'authentification des comptes uniquement par échange de clés de cryptographie asymétrique (**duo clé privée/publique**). Ces clés doivent être générées de préférence avant le déploiement du service. Elles permettent de s'authentifier sans avoir à saisir de mot de passe, ce qui complique toute tentative d'espionnage de ces mots de passe.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Dans l'idéal, se connecter avec un système de chiffrement par clé RSA au lieu de mot de passe.

# Pour finir, le service FTP est à remplacé par SFTP afin d'éviter la fuite d'informations par écoute du réseau via un "sniffer" sur le LAN. SFTP ( FTP via SSH ) utilise des algorithmes renforcés tels qu'AES et Triple DES pour chiffrer les données transférées, et offre ainsi un haut niveau de protection. Avec l'application de la recommandation précédente, SFTP est donc un service avec durcissement avancée de la sécurité pour tout transfert de fichiers sur le serveur web.

**RECOMMANDATION-CRITICAL** (défense en profondeur) : Remplacer FTP par SFTP pour un durcissement avancée de la sécurité de transfert de fichiers

## C - Approfondir avec des logiciels d'audit

### 1- Lynis

Il est normal et plutôt rassurant de retrouver beaucoup de nos recommandations dans les résultats de Lynis. Cependant, nous avons pu constater quelques différences : des ajouts, mais aussi des points moins détaillés chez Lynis. Un outil d'audit automatique tel que Lynis est là pour accompagner uniquement.

## [+] Initializing program

- Detecting OS... [ DONE ]

```
-----  
Program version:      2.1.1  
Operating system:    Linux  
Operating system name:  Ubuntu  
Operating system version: 16.04  
Kernel version:      4.4.0  
Hardware platform:    x86_64  
Hostname:             vm-audit  
Auditor:              [Unknown]  
Profile:              /etc/lynis/default.prf  
Log file:             /var/log/lynis.log  
Report file:         /var/log/lynis-report.dat  
Report version:      1.0  
Plugin directory:    /etc/lynis/plugins  
-----
```

## [+] Debian Tests

```
-----  
- Checking for system binaries that are required by Debian Tests...  
  - Checking /bin... [ FOUND ]  
  - Checking /sbin... [ FOUND ]  
  - Checking /usr/bin... [ FOUND ]  
  - Checking /usr/sbin... [ FOUND ]  
  - Checking /usr/local/bin... [ FOUND ]  
  - Checking /usr/local/sbin... [ FOUND ]  
- Authentication:  
  - PAM (Pluggable Authentication Modules):  
    - libpam-tmpdir [ Not Installed ]  
    - libpam-usb [ Not Installed ]  
- File System Checks:  
  - DM-Crypt, Cryptsetup & Cryptmount:  
    - Checking / on /dev/sda5 [ NOT ENCRYPTED ]  
    - Checking /boot on /dev/sda1 [ NOT ENCRYPTED ]  
  - Ecryptfs [ NOT INSTALLED ]  
- Software:  
  - apt-listbugs [ Not Installed ]  
  - apt-listchanges [ Not Installed ]  
  - checkrestart [ Not Installed ]  
  - debsecan [ Not Installed ]  
  - debsums [ Not Installed ]  
  - fail2ban [ Installed with jail.conf ]
```

( apt-listbugs & apt-listchanges, debsecan et debsums sont des packages propres à la distribution Debian, pas important dans notre Audit )

## [+] Boot and services

- Service Manager [ UNKNOWN ]
- Checking presence GRUB [ OK ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ WARNING ]
- Check running services (systemctl) [ DONE ]
  - Result: found 25 running services
- Check enabled services at boot (systemctl) [ DONE ]
  - Result: found 30 enabled services
- Check startup files (permissions) [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

## [+] Kernel

- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE)
  - CPU support: PAE and/or NoeXecute supported [ FOUND ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules [ DONE ]
  - Found 78 active modules
- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ FOUND ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration [ DISABLED ]
  - Checking setuid core dumps configuration [ PROTECTED ]
- Check if reboot is needed [ NO ]

## [+] Memory and processes

- Checking /proc/meminfo [ FOUND ]
- Searching for dead/zombie processes [ OK ]
- Searching for IO waiting processes [ OK ]



## [+] Users, Groups and Authentication

- Search administrator accounts [ OK ]
- Checking for non-unique UIDs [ OK ]
- Checking consistency of group files (grpck) [ OK ]
- Checking non unique group ID's [ OK ]
- Checking non unique group names [ OK ]
- Checking password file consistency [ WARNING ]
- Query system users (non daemons) [ DONE ]
- Checking NIS+ authentication support [ NOT ENABLED ]
- Checking NIS authentication support [ NOT ENABLED ]
- Checking sudoers file [ FOUND ]
  - Check sudoers file permissions [ OK ]
- Checking PAM password strength tools [ SUGGESTION ]
- Checking PAM configuration files (pam.conf) [ FOUND ]
- Checking PAM configuration files (pam.d) [ FOUND ]
- Checking PAM modules [ FOUND ]
- Checking LDAP module in PAM [ NOT FOUND ]
- Checking accounts without expire date [ OK ]
- Checking accounts without password [ OK ]
- Checking user password aging [ DISABLED ]
- Determining default umask
  - Checking umask (/etc/profile) [ OK ]
  - Checking umask (/etc/login.defs) [ SUGGESTION ]
  - Checking umask (/etc/init.d/rc) [ SUGGESTION ]
- Checking LDAP authentication support [ NOT ENABLED ]

## [+] Shells

- Checking shells from /etc/shells  
Result: found 6 shells (valid shells: 6).
  - Session timeout settings/tools [ NONE ]

## [+] File systems

- Checking mount points
  - Checking /home mount point [ SUGGESTION ]
  - Checking /tmp mount point [ SUGGESTION ]
  - Checking /var mount point [ OK ]
- Checking LVM volume groups
  - Checking LVM volumes [ FOUND ]
- Querying FFS/UFS mount points (fstab) [ NONE ]
- Query swap partitions (fstab) [ OK ]
- Testing swap partitions [ OK ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Checking Locate database [ FOUND ]

## [+] Storage

- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking firewire ohci driver (modprobe config) [ DISABLED ]

### [+] Name services

- Checking default DNS search domain [ NONE ]
- Checking /etc/resolv.conf options [ NONE ]
- Searching DNS domain name [ FOUND ]
  - Domain name: vm-audit
- Checking nscd status [ NOT FOUND ]
- Checking BIND status [ FOUND ]
  - Checking BIND configuration file [ FOUND ]
  - Checking BIND configuration consistency [ OK ]
  - Checking BIND version in banner [ WARNING ]
- Checking PowerDNS status [ NOT FOUND ]
- Checking ypbind status [ NOT FOUND ]
- Checking /etc/hosts
  - Checking /etc/hosts (duplicates) [ OK ]
  - Checking /etc/hosts (hostname) [ OK ]
  - Checking /etc/hosts (localhost) [ OK ]

### [+] Ports and packages

- Searching package managers
  - Searching RPM package manager [ FOUND ]
    - Querying RPM package manager
  - Searching dpkg package manager [ FOUND ]
    - Querying package manager
- Query unpurged packages [ NONE ]
- Checking YUM package management consistency [ WARNING ]
- yum-utils package not installed [ SUGGESTION ]
- Checking missing security packages [ SKIPPED ]
- Checking security repository in sources.list file [ OK ]
- Checking APT package database [ OK ]

### [+] Ports and packages

- Searching package managers
    - Searching RPM package manager [ FOUND ]
      - Querying RPM package manager
    - Searching dpkg package manager [ FOUND ]
      - Querying package manager
  - Query unpurged packages [ NONE ]
  - Checking YUM package management consistency [ WARNING ]
  - yum-utils package not installed [ SUGGESTION ]
  - Checking missing security packages [ SKIPPED ]
  - Checking security repository in sources.list file [ OK ]
  - Checking APT package database [ OK ]
  
  - Checking vulnerable packages [ WARNING ]
  - Checking upgradeable packages [ SKIPPED ]
  - Checking package audit tool [ INSTALLED ]
- Found: apt-get

( Yum n'est pas à prendre en compte sur une machine ubuntu mais RedHat ) Désinstallation de Yum

## [+] Networking

- ```
-----  
- Checking configured nameservers  
  - Testing nameservers  
    Nameserver: 172.20.10.1 [ OK ]  
  - Minimal of 2 responsive nameservers [ WARNING ]  
- Checking default gateway [ DONE ]  
- Getting listening ports (TCP/UDP) [ DONE ]  
  * Found 19 ports  
- Checking promiscuous interfaces [ OK ]  
- Checking waiting connections [ OK ]  
- Checking status DHCP client [ RUNNING ]
```

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

## [+] Printers and Spools

- ```
-----  
- Checking cups daemon [ NOT FOUND ]  
- Checking lp daemon [ NOT RUNNING ]
```

## [+] Software: e-mail and messaging

- ```
-----  
- Checking Exim status [ NOT FOUND ]  
- Checking Postfix status [ RUNNING ]  
- Checking Postfix configuration [ FOUND ]  
  - Checking Postfix banner [ WARNING ]  
- Checking Dovecot status [ RUNNING ]  
- Checking Qmail status [ NOT FOUND ]  
- Checking Sendmail status [ NOT FOUND ]
```

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

## [+] Software: firewalls

- ```
-----  
- Checking iptables kernel module [ FOUND ]  
  - Checking for empty ruleset [ OK ]  
  - Checking for unused rules [ OK ]  
  - Checking pflogd status [ NOT FOUND ]  
- Checking pf [ NOT FOUND ]  
- Checking host based firewall [ ACTIVE ]
```

### [+] Software: webservers

- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]
  - Info: No virtual hosts found
  - \* Loadable modules [ FOUND ]
    - Found 106 loadable modules
    - mod\_evasive: anti-DoS/brute force [ NOT FOUND ]
    - mod\_qos: anti-Slowloris [ NOT FOUND ]
    - mod\_spamhaus: anti-spam (spamhaus) [ NOT FOUND ]
    - ModSecurity: web application firewall [ NOT FOUND ]
- Checking nginx [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] SSH Support

- Checking running SSH daemon [ FOUND ]
  - Searching SSH configuration [ FOUND ]
  - Checking defined SSH options [ DONE ]
    - SSH option: PermitRootLogin [ WARNING ]
    - SSH option: Protocol [ OK ]
    - SSH option: StrictModes [ OK ]
    - SSH option: AllowUsers [ NOT FOUND ]
    - SSH option: AllowGroups [ NOT FOUND ]

### [+] SNMP Support

- Checking running SNMP daemon [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Databases

- MySQL process status [ FOUND ]
  - Checking empty MySQL root password [ WARNING ]
- PostgreSQL processes status [ NOT FOUND ]
- Oracle processes status [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] LDAP Services

- Checking OpenLDAP instance [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] PHP

- Checking PHP [ NOT FOUND ]

### [+] Squid Support

-----  
- Checking running Squid daemon [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Logging and files

-----  
- Checking for a running log daemon [ OK ]  
- Checking Syslog-NG status [ NOT FOUND ]  
- Checking systemd journal status [ FOUND ]  
- Checking Metalog status [ NOT FOUND ]  
- Checking RSyslog status [ FOUND ]  
- Checking RFC 3195 daemon status [ NOT FOUND ]  
- Checking minilogd instances [ NOT FOUND ]  
- Checking logrotate presence [ OK ]  
- Checking log directories (static list) [ DONE ]  
- Checking open log files [ DONE ]  
- Checking deleted files in use [ FILES FOUND ]

### [+] Banners and identification

-----  
- /etc/motd [ NOT FOUND ]  
- /etc/issue [ FOUND ]  
- /etc/issue contents [ WEAK ]  
- /etc/issue.net [ FOUND ]  
- /etc/issue.net contents [ WEAK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Scheduled tasks

-----  
- Checking crontab/cronjob [ DONE ]  
- Checking atd status [ RUNNING ]  
- Checking at users [ DONE ]  
- Checking at jobs [ NONE ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Accounting

- Checking accounting information [ NOT FOUND ]
- Checking sysstat accounting data [ NOT FOUND ]
- Checking auditd [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Time and Synchronization

- Checking event based ntpdate (if-up) [ FOUND ]
- Checking for a running NTP daemon or client [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Cryptography

- Checking SSL certificate expiration [ WARNING ]

### [+] Security frameworks

- Checking presence AppArmor [ FOUND ]
  - Checking AppArmor status [ ENABLED ]
- Checking presence SELinux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Software: file integrity

- Checking file integrity tools
- Checking presence integrity tool [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

### [+] Software: System tooling

- Checking automation tooling
- Automation tooling [ NOT FOUND ]

[+] **Software: Malware scanners**

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] **File Permissions**

```
- Starting file permissions check
  /etc/lilo.conf           [ NOT FOUND ]
  /root/.ssh              [ NOT FOUND ]
```

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] **Home directories**

```
- Checking shell history files           [ OK ]
```

[+] **Kernel Hardening**

```
- Comparing sysctl key pairs with scan profile
  - kernel.core_uses_pid (exp: 1)       [ DIFFERENT ]
  - kernel.ctrl-alt-del (exp: 0)       [ OK ]
  - kernel.kptr_restrict (exp: 1)      [ OK ]
  - kernel.sysrq (exp: 0)              [ DIFFERENT ]
  - net.ipv4.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
  - net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
  - net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
  - net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
  - net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
  - net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
  - net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
  - net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.accept_source_route (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
  - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
  - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
  - net.ipv4.tcp_syncookies (exp: 1)    [ OK ]
  - net.ipv4.tcp_timestamps (exp: 0)    [ DIFFERENT ]
  - net.ipv6.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
  - net.ipv6.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]
```

[+] **Hardening**

```
- Installed compiler(s)           [ FOUND ]
- Installed malware scanner       [ NOT FOUND ]
```

### Warnings:

- Version of Lynis is very old and should be updated [test:NONE]  
<https://cisofy.com/controls/test:NONE/>
- pwck found one or more errors/warnings in the password file [AUTH-9228]  
<https://cisofy.com/controls/AUTH-9228/>
- Found BIND version in banner [NAME-4210]  
<https://cisofy.com/controls/NAME-4210/>
- YUM is not properly configured or registered for this platform (no repolist found) [PKGS-7383]  
<https://cisofy.com/controls/PKGS-7383/>
- Found one or more vulnerable packages. [PKGS-7392]  
<https://cisofy.com/controls/PKGS-7392/>
- Couldn't find 2 responsive nameservers [NETW-2705]  
<https://cisofy.com/controls/NETW-2705/>
- Found mail\_name in SMTP banner, and/or mail\_name contains 'Postfix' [MAIL-8818]  
<https://cisofy.com/controls/MAIL-8818/>
- Root can directly login via SSH [SSH-7412]  
<https://cisofy.com/controls/SSH-7412/>
- No MySQL root password set [DBS-1816]  
<https://cisofy.com/controls/DBS-1816/>

### Suggestions:

- Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions [CUST-0280]  
<https://your-domain.example.org/controls/CUST-0280/>
- Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]  
<https://your-domain.example.org/controls/CUST-0285/>
- Install 'cryptfs-utils' and configure for each user. [CUST-0520]  
<https://your-domain.example.org/controls/CUST-0520/>
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]  
<https://your-domain.example.org/controls/CUST-0810/>
- Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]  
<https://your-domain.example.org/controls/CUST-0811/>
- Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]  
<https://your-domain.example.org/controls/CUST-0830/>
- Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]  
<https://your-domain.example.org/controls/CUST-0870/>
- Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]  
<https://your-domain.example.org/controls/CUST-0875/>
- Copy /etc/fail2ban/jail.conf to jail.local to prevent it being changed by updates. [DEB-0880]  
<https://cisofy.com/controls/DEB-0880/>
- Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]  
<https://cisofy.com/controls/BOOT-5122/>
- Determine runlevel and services at startup [BOOT-5180]  
<https://cisofy.com/controls/BOOT-5180/>
- Run pwck manually and correct found issues. [AUTH-9228]  
<https://cisofy.com/controls/AUTH-9228/>
- Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]  
<https://cisofy.com/controls/AUTH-9262/>
- Configure password aging limits to enforce password changing on a regular base [AUTH-9286]  
<https://cisofy.com/controls/AUTH-9286/>

- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  
<https://cisofy.com/controls/AUTH-9328/>
- Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]  
<https://cisofy.com/controls/AUTH-9328/>
- To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]  
<https://cisofy.com/controls/FILE-6310/>
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]  
<https://cisofy.com/controls/FILE-6310/>
- Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]  
<https://cisofy.com/controls/STRG-1840/>
- The version in BIND can be masked by defining 'version none' in the configuration file [NAME-4210]  
<https://cisofy.com/controls/NAME-4210/>
- Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]  
<https://cisofy.com/controls/PKGS-7308/>
- Install debsums utility for the verification of packages with known good database. [PKGS-7370]  
<https://cisofy.com/controls/PKGS-7370/>
- Install package 'yum-utils' for better consistency checking of the package database [PKGS-7384]  
<https://cisofy.com/controls/PKGS-7384/>
- Install package yum-plugin-security if possible, to maintain security updates easier (yum install yum-plugin-security) [PKGS-7386]  
<https://cisofy.com/controls/PKGS-7386/>
- Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]  
<https://cisofy.com/controls/PKGS-7392/>
- Install package apt-show-versions for patch management purposes [PKGS-7394]  
<https://cisofy.com/controls/PKGS-7394/>
- Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]  
<https://cisofy.com/controls/NETW-2705/>
- You are advised to hide the mail\_name (option: smtpd\_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]  
<https://cisofy.com/controls/MAIL-8818/>
- Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]  
<https://cisofy.com/controls/HTTP-6640/>
- Install Apache mod\_qos to guard webserver against Slowloris attacks [HTTP-6641]



```

https://cisofy.com/controls/HTTP-6641/
- Install Apache mod_spamhaus to guard webserver against spammers [HTTP-6642]
  https://cisofy.com/controls/HTTP-6642/
- Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
  https://cisofy.com/controls/HTTP-6643/
- Use mysqladmin to set a MySQL root password (mysqladmin -u root -p password MYPASSWORD) [DBS-1816]
  https://cisofy.com/controls/DBS-1816/
- Check what deleted files are still in use and why. [LOGG-2190]
  https://cisofy.com/controls/LOGG-2190/
- Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
  https://cisofy.com/controls/BANN-7126/
- Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
  https://cisofy.com/controls/BANN-7130/
- Enable process accounting [ACCT-9622]
  https://cisofy.com/controls/ACCT-9622/
- Enable sysstat to collect accounting (no results) [ACCT-9626]
  https://cisofy.com/controls/ACCT-9626/
- Enable auditd to collect audit information [ACCT-9628]
  https://cisofy.com/controls/ACCT-9628/
- Check available certificates for expiration [CRYP-7902]
  https://cisofy.com/controls/CRYP-7902/
- Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
  https://cisofy.com/controls/FINT-4350/
- Determine if automation tools are present for system management [TOOL-5002]
  https://cisofy.com/controls/TOOL-5002/
- One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
  https://cisofy.com/controls/KRNL-6000/
- Harden compilers like restricting access to root user only [HRDN-7222]
  https://cisofy.com/controls/HRDN-7222/
- Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
  https://cisofy.com/controls/HRDN-7230/

```

## Lynis security scan details:

```

Hardening index : 50 [#####]
Tests performed : 211
Plugins enabled : 1

```

### Quick overview:

```
- Firewall [V] - Malware scanner [X]
```

### Lynis Modules:

```
- Heuristics Check [NA] - Security Audit [V]
- Compliance Tests [X] - Vulnerability Scan [V]
```

## D - Rapport d'audit et préconisations

### 1 - Tableaux du bilan d'audit & recommandations

#### Analyse externe

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Interdire l'ouverture du port 3306 vers l'extérieur ( Sauf si un serveur Apache externe doit s'y connecter )	CRITIQUE	Défense en profondeur	Audit Manuel
Cacher la version des services visibles depuis un scan réseau externe	CRITIQUE	Défense en profondeur	Audit Manuel

## L'intégrité et la mise à jour des packages installés

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier que l'ensemble des packages installés sur le système sont signés et sûrs avec les attributs gpgcheck et gpgkey	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier que l'ensemble des mises à jour de sécurités et dernières versions des packages sont installés.	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier la planification régulière d'une tâche automatique pour mettre à jour les packages corrigés pour raisons de sécurité	CRITIQUE	Défense en profondeur	Audit Manuel
Mise à jour certificat SSL ( Dans une utilisation hypothétique de FTPS )	ATTENTION	Défense en profondeur	Audit Lynis

## Bootloader, les options du noyau et ses modules

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
passer les droits sur l'arborescence /etc/grub.d/ à 700	CRITIQUE	moins de privilège	Audit Manuel
Créer un utilisateur et son mot de passe chiffré dans le fichier 01_users afin de protéger l'accès au shell de Grub par une authentification	CRITIQUE	minimisation	Audit Manuel
passer l'option rhgb et quiet aux variables GRUB_CMD_LINUX_DEFAULT & GRUB_CMD_LINUX	ATTENTION	minimisation	Audit Manuel
passer l'option iommu=force au noyau lors du démarrage de Linux	ATTENTION	minimisation	Audit Manuel
Bloquer le chargement de modules supplémentaires via la sysctl kernel.modules_disabled=1 Veiller à intégrer les modules non	ATTENTION	minimisation	Audit Manuel

dynamiquement par recompilation du noyau ( Attention aux serveurs applicatifs qui nécessitent de nouveaux modules )			
Installation de grsecurity augmentant la sécurité du noyau	ATTENTION	Défense en profondeur	Audit Lynis
définir les options de durcissement du kernel ( si le serveur n'est pas un routeur uniquement ! ) :  kernel.core_uses_pid = 1 kernel.sysrq = 0 net.ipv4.conf.all.accept_redirect = 0 net.ipv4.conf.all.log_martians = 0 net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv4.conf.default.accept_source_route = 0 net.ipv4.conf.default.log_martians = 1 net.ipv4.tcp_timestamps = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_source_route = 0	ATTENTION	Défense en profondeur	Audit Lynis

### Les consoles virtuelles

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Videz le contenu tty1 à tty63 du fichier /etc/securetty afin de bloquer toute connexion avec l'utilisateur root depuis une console virtuelle	CRITIQUE	Défense en profondeur	Audit Manuel
Augmenter l'intervalle de temps entre chaque tentative de connexion sur le module pam_faildelay.so afin de ralentir les attaques par dictionnaire ( anti-robot)	ATTENTION	Défense en profondeur	Audit Manuel
Désactivez la combinaison Ctrl+Alt+Supp sur le serveur pour	CRITIQUE	Défense en profondeur	Audit Manuel

prévenir tout redémarrage depuis un accès physique à la machine

### Le mode de démarrage du serveur

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Changer la cible par défaut avec un service non graphique : multi-user.target	ATTENTION	minimisation	Audit Manuel
Supprimer les cibles inutiles comme sound.target & graphical.target ( Attention ce dernier doit être supprimé que si aucun GUI ne sera installé ) Si le serveur n'est pas un serveur de messagerie alors mail-transport-agent.target peut également être supprimé.	ATTENTION	minimisation	Audit Manuel
Supprimer les services cibles inutiles démarrés automatiquement avec le serveur comme atd.service ( car cron.service déjà présent. dovecot.service ( uniquement si le serveur web n'utilise pas de service messagerie configurable avec imap/pop ) Ajouter accounts-daemon.service ( service chargé par défaut du graphical.target remplacé par multi-user.target )	CRITIQUE	minimisation	Audit Manuel

### Les composants matériels

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier que le CPU dispose bien des flags PAE et NX	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier la présence d'un minimum de mémoire SWAP sur le système	ATTENTION	Défense en profondeur	Audit Manuel

## Le partitionnement des disques

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier le chiffrement des partitions sensibles du système	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier que le partitionnement isole et protège les composants du système ( /boot ; /tmp ; /home ; /var ; /var/log ; )	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier les options de montage suivants pour les répertoires /tmp ( rw, nosuid, nodev, noexec ) /home ( rw, nosuid, nodev, noexec ) /var ( rw, nosuid, nodev, noexec, sync ) /var/log ( rw, nosuid, nodev, noexec, sync )	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier la protection de la partition /boot	CRITIQUE	moins de privilège	Audit Manuel

## Les comptes utilisateurs, les mots de passes, les droits spéciaux et les mises à jours de sécurité

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier la robustesse des mots de passe en installant et configurant le module pam_pwquality	ATTENTION	Défense en profondeur	Audit Manuel
Installer les modules d'authentification sécurisés libpam-tmpdir & libpam-usb	ATTENTION	Défense en profondeur	Audit Lynis
Vérifier que les comptes utilisateurs qui peuvent se connecter ont pour obligation de changer leur mot de passe régulièrement	CRITIQUE	Défense en profondeur	Audit Manuel

Vérifier les valeurs par défaut des attributs des mots de passe pour chaque compte utilisateur dans /etc/login.defs	ATTENTION	Défense en profondeur	Audit Manuel
Vérifier les valeurs par défaut des attributs des mots de passe pour chaque compte utilisateur dans /etc/init.d/rc	ATTENTION	Défense en profondeur	Audit Lynis
Vérifier que l'utilisateur Daniel existe pour l'entreprise sinon prendre les mesures pour s'informer des derniers événements de l'utilisateur et supprimer définitivement son accès.	CRITIQUE	Défense en profondeur	Audit Manuel
Examiner et maîtriser la liste des fichiers avec les droits spéciaux setuid, setgid et sticky bit	CRITIQUE	moins privilège	Audit Manuel
Vérifier la présence d'un groupe d'utilisateurs identifié comme administrateur de la machine et disposant des droits de changement de privilèges par l'intermédiaire d'un processus type sudo	CRITIQUE	moins privilège	Audit Manuel
Vérifier que la commande sudo peut être exécutée uniquement par le groupe administrateur (+ root)	CRITIQUE	moins privilège	Audit Manuel
Vérifier que le fichier de configuration /etc/sudoers contient la déclaration des commandes nécessaires au maintien du système pour les utilisateurs du groupe administrateur	CRITIQUE	moins privilège	Audit Manuel
Installation de SELinux pour mieux contrôler les accès au système	ATTENTION	Défense en profondeur	Audit Lynis

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier et appliquer le durcissement de la configuration des services lancés	CRITIQUE	Défense en profondeur	Audit Manuel
Vérifier que le mot de passe root mysql n'est pas vide	CRITIQUE	Défense en profondeur	Audit Lynis
Désactiver le versionning banner pour bind & postfix ( même recommandation que analyse externe )	CRITIQUE	Défense en profondeur	Audit Lynis

### Le cloisonnement des services lancés

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier les comptes système associés aux services	CRITIQUE	moins privilège	Audit Manuel
Vérifiez les droits du système de fichiers associé aux comptes système exécutant des services	CRITIQUE	moins privilège	Audit Manuel
Vérifier qu'il est possible de virtualiser l'architecture applicative du serveur	ATTENTION	Défense en profondeur	Audit Manuel
Vérifier que le chrootage est utilisé sur les services lancés dans la mesure du possible	CRITIQUE	Défense en profondeur	Audit Manuel

### Les fichiers de trace des services

<u>Recommandation</u>	<u>Type</u>	<u>Principe</u>	<u>Méthode</u>
Vérifier le cloisonnement du service Syslog	CRITIQUE	Défense en profondeur	Audit Manuel
Mettre en place le processus de supervision des fichiers de trace	ATTENTION	Défense en profondeur	Audit Manuel

## Les ports ouverts du serveur et les processus associés

Recommandation	Type	Principe	Méthode
Désactiver le service DHCP et adresser le réseau manuellement pour le serveur. Dans la mesure du possible, réduire le masque de sous réseau aux besoins exact d'adresse IP. ( Prendre en compte la scalabilité de l'entreprise si croissance rapide )	CRITIQUE	minimisation	Audit Manuel
Désactiver le port 3306 en écoute depuis l'extérieur pour le service de base de donnée.	CRITIQUE	minimisation	Audit Manuel
Vérifiez que les ports par défaut des services ont été changés dans la mesure du possible	ATTENTION	Défense en profondeur	Audit Manuel

## Les processus de filtrage réseau, pare feu et proxy

Recommandation	Type	Principe	Méthode
Vérifier que les TCP Wrappers sont configurés pour les services réseau compatibles	CRITIQUE	Défense en profondeur	Audit Manuel
Installer le filtre réseau pflogd	ATTENTION	Défense en pr	Audit Lynis
Vérifier qu'il est possible d'accéder au firewall Netfilter par le noyau sans la contrainte module	ATTENTION	minimisation	Audit Manuel
Vérifier et appliquer que les règles Netfilter sont bien positionnées pour les configurations par défauts et les services du serveur web.	CRITIQUE	Défense en profondeur	Audit Manuel
Dans la mesure du possible, cloisonner les services du serveur	CRITIQUE	Défense en profondeur	Audit Manuel



web et appliquer des règles FORWARD sur un plan d'adressage définit pour chaque service			
Vérifier le positionnement des sysctl réseau communes au noyau dans le fichier /etc/sysctl.conf	CRITIQUE	Défense en profondeur	Audit Manuel
Installation anti malware & anti rootkits logiciels avec scan périodique	ATTENTION	Défense en profondeur	Audit Lynis

### Les services ssh et ftp

Recommandation	Type	Principe	Méthode
Restreindre la directive PermitRootLogin du service SSH	CRITIQUE	moins de privilège	Audit Manuel
Changer le port d'écoute par défaut du service SSH	CRITIQUE	Défense en profondeur	Audit Manuel
Appliquer un blocage idle et tracer les tentatives de connexions échouées	CRITIQUE	Défense en profondeur	Audit Manuel
Dans l'idéal, se connecter avec un système de chiffrement par clé RSA au lieu de mot de passe.	CRITIQUE	Défense en profondeur	Audit Manuel
Remplacer FTP par SFTP pour un durcissement avancé de la sécurité de transfert de fichiers	CRITIQUE	Défense en profondeur	Audit Manuel

## 2 - Préconisations additionnelles

### a) Politique de sécurité du SI au sein de l'entreprise

Une **politique de sécurité des systèmes d'information (PSSI)** reflète la **vision stratégique** de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme ;

Concrètement, on y trouve :

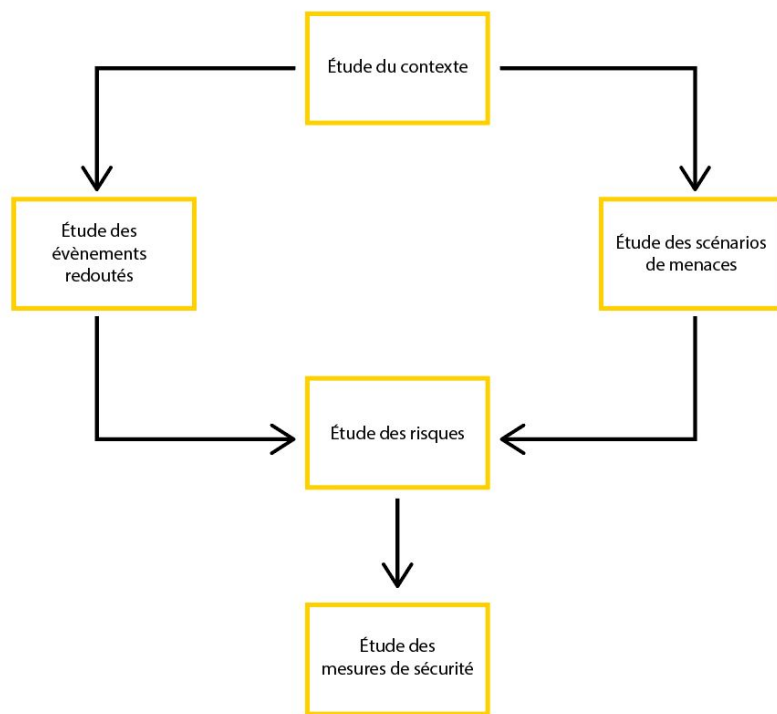
- la définition des **enjeux** d'une PSSI au regard de l'entreprise, son champ d'application et un **inventaire** des biens (physiques mais aussi organisationnels) à protéger
- une **analyse** du **contexte réglementaire** de l'entreprise et des **risques** qui pèsent sur le SI,
- la déclinaison des enjeux précédents en **exigences** et **mesures de sécurité**.

Dans ce panorama complexe, le SI doit assurer la méthode DICT : **confidentialité, intégrité, disponibilité** et la **traçabilité** des données.

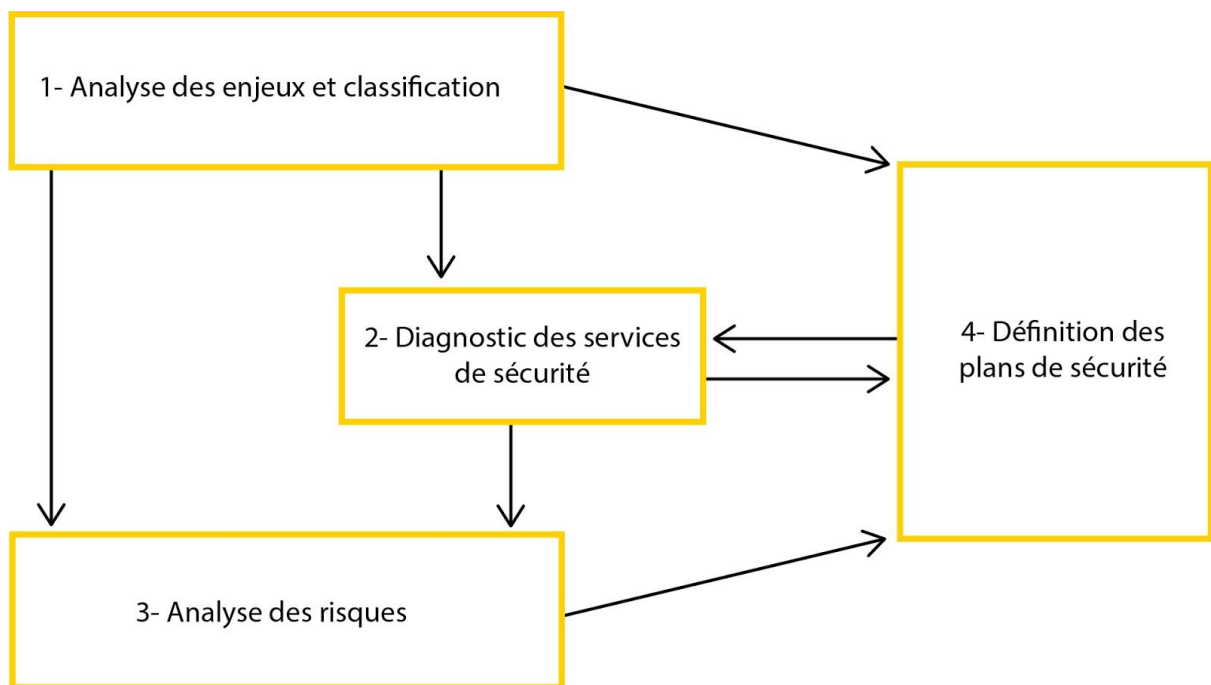
L'industrie de la sécurité informatique recommande aux DSI et aux chefs de projet un ensemble de **standards** et de **bonnes pratiques** pour réaliser leurs travaux de sécurisation des SI. L'application de ces normes garantit un **cadre éprouvé** et **reconnu** pour déployer une PSSI. L'écosystème le plus répandu est l'ensemble des **normes ISO**.

Normes	Date et révision	Descriptif	Lien avec la PSSI
<b>ISO 27001</b>	2005 - 2013	Ce standard définit les exigences à mettre en place pour l'élaboration d'un système de management de la sécurité de l'information. Basé sur l'amélioration continue de type « roue de Deming » Plan / Do / Check / Act, il précise les points de contrôle à respecter et propose dans son annexe A 114 mesures issues de l'ISO 27002.	C'est la base pour la mise en place d'un SMSI (système de management de la sécurité de l'information).
<b>ISO 27002</b>	2005 - 2013	Ce standard présente un guide de bonnes pratiques à mettre en oeuvre pour des contrôles au regard des risques pesant sur l'information (confidentialité, intégrité et disponibilités). Il présente 114 mesures classées en 14 thèmes.	La méthodologie présentée dans le cours s'inspire directement des thèmes de l'ISO 27002 pour fixer les exigences et règles de sécurité.
<b>ISO 27003</b>	2010 - 2017	Cette norme présente un guide d'implémentation d'un SMSI. Il décrit le processus de conception.	Base pour la mise en place d'un SMSI.
<b>ISO 27005</b>	2008- 2018	Cette norme se focalise sur la gestion des risques : définition du contexte, évaluation des risques, contrôle des résultats, révision. Par exemple, les méthodes EBIOS et MEHARI se basent de manière extensive sur la norme 27005.	Pas de lien direct, mais la PSSI se nourrit d'une analyse des risques qui peut s'appuyer sur l'ISO 27005. C'est même recommandé. 😊

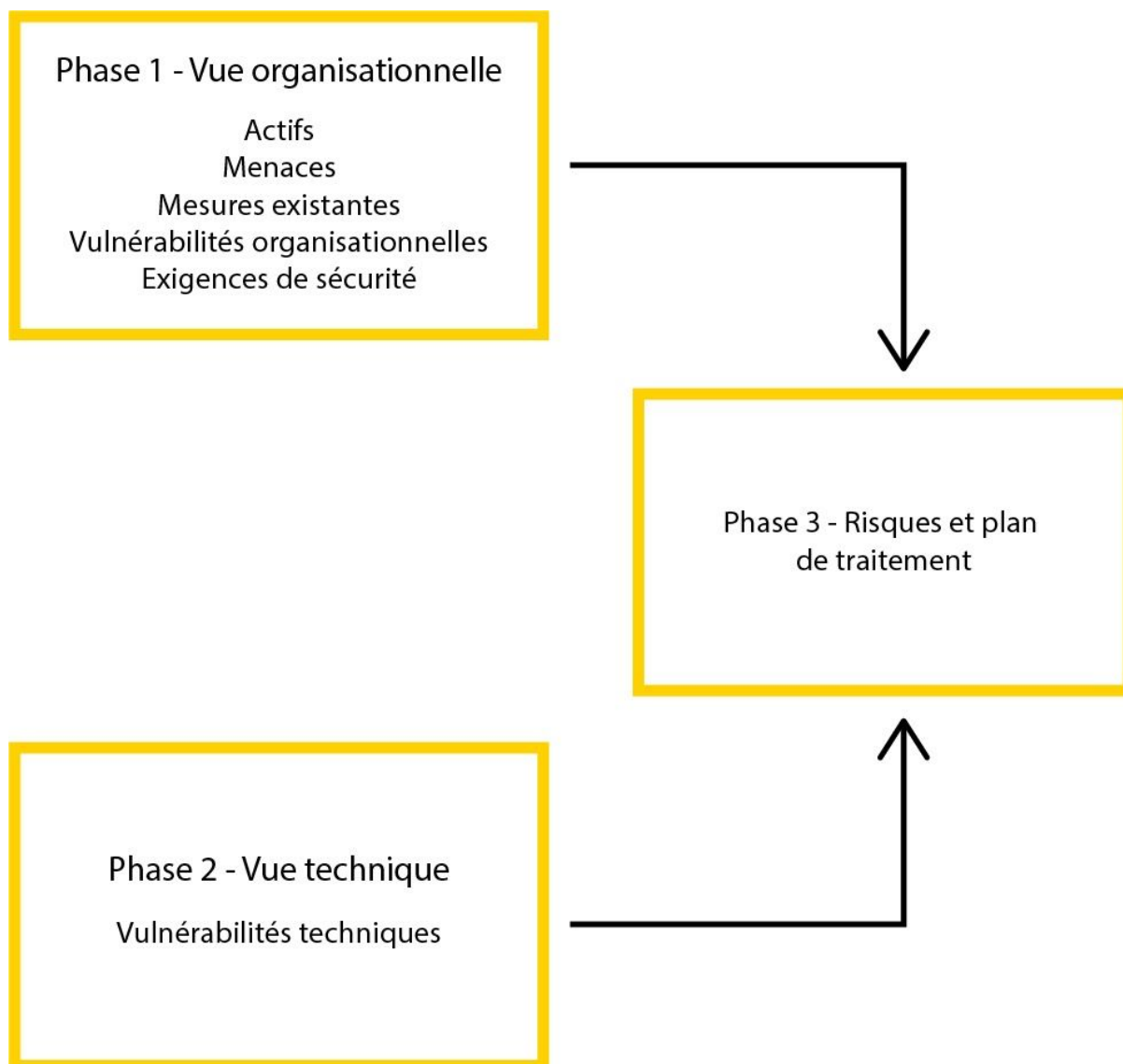
### Exemple de la méthodologie EBIOS ISO 27005 :



### Exemple de la méthodologie MEHARI ISO 27005



### Exemple de la méthodologie OCTAVE ISO 27005



Il faut donc envisager les normes ISO comme un référentiel d'objectifs, une proposition de méthodologie, qui doivent toutefois être enrichis du bon sens et de l'expertise des professionnels de la SSI.

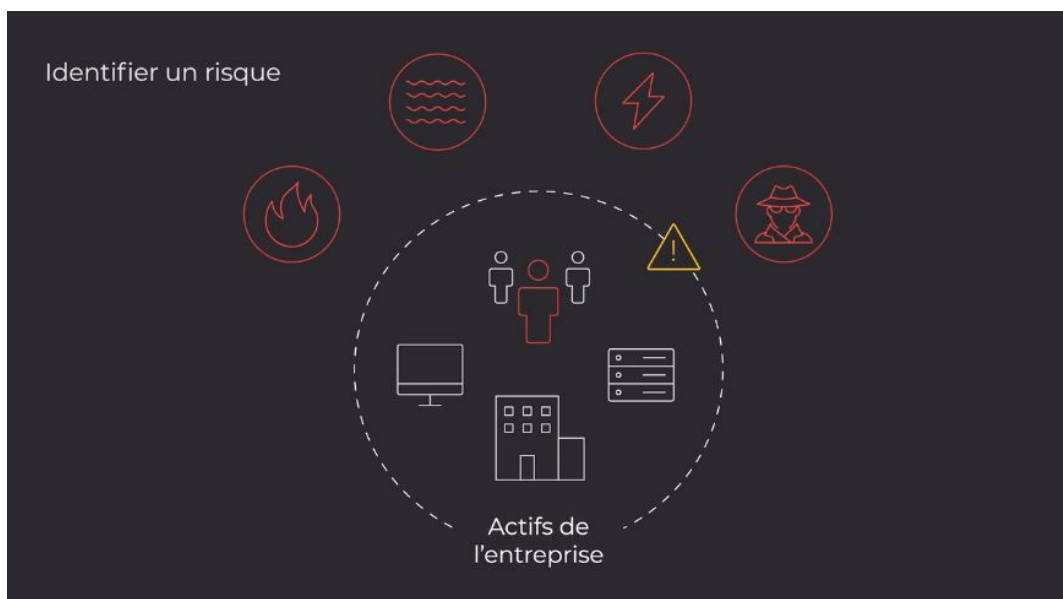
La méthode proposée à l'élaboration de la PSSI se décompose en 4 phases principales :

- **cadrer la démarche** : Analyser votre contexte professionnel, Élaborer l'introduction au document engageant la **direction** dans la stratégie SSI globale, Formuler les enjeux et le champ d'application de la PSSI, Fixer le cadre légal et réglementaire, ainsi que les obligations contractuelles ( voir d )

- **recenser les biens** à protéger : La phase de bilan des biens vise à déterminer les éléments du **patrimoine matériel** et **organisationnel** ( les actifs de l'entreprise ) que les règles de la PSSI vont contribuer à protéger, pour permettre à la structure de mener ses activités ;

Il ne s'agit pas de répertorier finement les matériels au sens d'une gestion logistique, il ne s'agit pas de répertorier finement les matériels au sens d'une gestion logistique, mais plutôt d'**identifier les groupes de composants semblables** dont la responsabilité incombe à un **acteur unique**

- **analyser les risques** : Une méthode d'analyse de risque permet d'établir un **tableau récapitulatif des risques**, de décrire leur **vraisemblance** et leur **gravité** pour l'ensemble des actifs de l'entreprise ; L'appréciation des risques se cadence en trois étapes : 1- **Identifier** ; 2- **Analyser** ; 3- **Évaluer** ;



Identifier les menaces :

Type de menaces	Exemples
Dommages physiques	Feu
	Dégât d'eau
Désastre naturel	Phénomène climatique
	Inondation
Perte de services essentiels	Panne du système de climatisation
	Panne électrique
Perturbations dues à des rayonnements	Rayonnements électromagnétiques
	Rayonnements thermiques
Compromission d'information	Vol de supports ou de documents
	Données provenant de source non fiable
Défaillance technique	Panne de matériel
	Dysfonctionnement d'un logiciel
Actions non autorisées	Utilisation non autorisée du matériel
	Reproduction frauduleuse de logiciel
Compromission des fonctions	Usurpation de droit

### Identifier les vulnérabilités :

Type de vulnérabilité	Exemples
Matériel informatique	Maintenance insuffisante
	Stockage non protégé
Logiciel	Attribution erronée de droit d'accès
	Interface utilisateur compliquée
Réseau	Architecture réseau non sécurisée
	Point de défaillance unique
Personnel	Formation insuffisante
	Absence de personnel
Site (lieu)	Réseau électrique instable
	Site situé en zone inondable
Structure organisationnelle	Absence d'audits réguliers
	Absence de procédure d'accès aux ressources

La **probabilité d'occurrence** du scénario de risque.

Élément d'occurrence		Probabilité d'occurrence	
Expérience passée	Élément externe		
Ne s'est jamais produit	Pas d'événement similaire dans la presse spécialisée	Improbable	1
Se produit plusieurs fois dans l'année	Événement similaire dans la presse spécialisée	Possible	2
Se produit plusieurs fois par mois	Événement similaire dans la presse courante	Probable	3
Se produit plusieurs fois par semaine	Événement récurrent dans la presse courante	Fréquent	4

La **complexité d'exécution** du scénario de risque.

Complexité			Niveau de complexité	
Connaissance de la société	Connaissance technique	Conditions		
Personne externe à la société Absence de connaissance spécifique requise	Absence de connaissance requise	Environnement extrêmement favorable (pas de mesure de sécurité implémentée)	Facile	1
Personne externe avec une bonne connaissance de la société	Connaissance ou recherche nécessaire	Environnement favorable (pas de mesure de sécurité implémentée)	Moyen	2
Personne externe avec une très bonne connaissance de la société. Un ancien employé par exemple	Connaissance et recherche nécessaires	Mesure de sécurité implémentée	Difficile	3
Complicité interne obligatoire	Connaissance avancée et recherche nécessaires	Mesure de sécurité implémentée et efficace	Très difficile	4

En combinant ces deux notions, on aboutit à la **matrice de vraisemblance** ci-dessous :

Vraisemblance					
	Probabilité de l'occurrence	1	2	3	4
Complexité d'exploitation de la vulnérabilité	4	1	1	1	2
	3	1	2	2	3
	2	2	3	4	4
	1	2	3	4	4

Identifier les mesures existantes :



Dans le cas général, la maturité d'une mesure existante s'évalue sur **une échelle à 5 niveaux** :

- **0 - Inexistante** : pas de processus identifiable ;
- **1 - Initialisée** : problème reconnu mais pas d'approche standardisée ;
- **2 - Reproductible** : des processus existent et sont appliqués par des personnes différentes ;
- **3 - Définie** : procédures standardisées, documentées et communiquées ;
- **4 - Gérée** : le contrôle de la conformité aux procédures est réalisé ;
- **5 - Optimisée** : le processus d'amélioration continue est réalisé et documenté.

#### Identifier les conséquences :

On classe ces conséquences selon les critères de **disponibilité, intégrité et confidentialité**. Voici une liste de conséquences qui impactent un ou plusieurs de ces critères :

- pertes financières ;
- perte de clientèle ;
- perte de fournisseurs ;
- poursuites judiciaires ;
- perte d'avantage concurrentiel ;
- perte d'efficacité ;
- atteinte à la vie privée des clients ;
- interruption de service ;
- incapacité de fournir le service ;
- perte d'image de marque ;
- atteinte à la sécurité du personnel.

les conséquences de la réalisation d'un scénario de risque s'évaluent sur tous les plans : financier, juridique, parts de marché, relations fournisseurs, image de marque, sécurité du personnel, etc.

#### Classification simplifiée des risques :

Risque	Source	Impact	Gravité	Probabilité	Niveau de risque

- **choisir les mesures de sécurité** : Une première étape permet de **fixer les exigences de sécurité** exprimées de façon fonctionnelle et non technique, par thème abordé ;

Une seconde tâche consiste à décliner ces exigences en **règles opérationnelles** dont **la gestion des menaces** et à spécifier le **composant** du SI sur lequel elle s'applique, et son caractère éventuellement externalisable ;

La PSSI est complétée par des annexes importantes : au minimum, les **coordonnées des personnels** en charge d'une fonction sécurité dans l'entreprise, et des matrices de risques "synthèses" des scénarii .

Menace	Conséquence	Vraisemblance	Niveau de risque	Ordre de priorité de traitement
Scénario A	5	2	10	2
Scénario B	2	4	8	3
Scénario C	3	5	15	1
Scénario D	1	3	3	5
Scénario E	4	1	4	4
Scénario F	2	4	8	3

Probabilité d'occurrence	Gravité du dommage			
	1	2	3	4
	2	4	6	8
	3	6	9	12
4	8	12	16	

Il est également recommandé d'apporter un plan de traitement des scénarii pour période donnée :

Action	Priorité	Deadline	Ressources	Rôles
Chiffrer les disques hébergeant les modèles de tarification	Haute	Court terme (d'ici 3 mois)	* Logiciel de chiffrement	* Administrateur IT : sélection et mise en place du logiciel de chiffrement  * DSI : validation du logiciel choisi
Définir, documenter et communiquer un processus de gestion des droits d'accès aux modèles de tarification	Moyenne	Moyen terme (d'ici 6 mois)	* Outil de gestion des droits d'accès	* Administrateur IT : sélection, mise en place et documentation du processus de gestion des droits d'accès  *DSI : validation du processus
Vérification du passé professionnel des nouvelles recrues	Basse	Long terme (d'ici 12 mois)	* NA	* Recruteurs: définition d'actions de vérification des passés professionnels des personnes recrutées

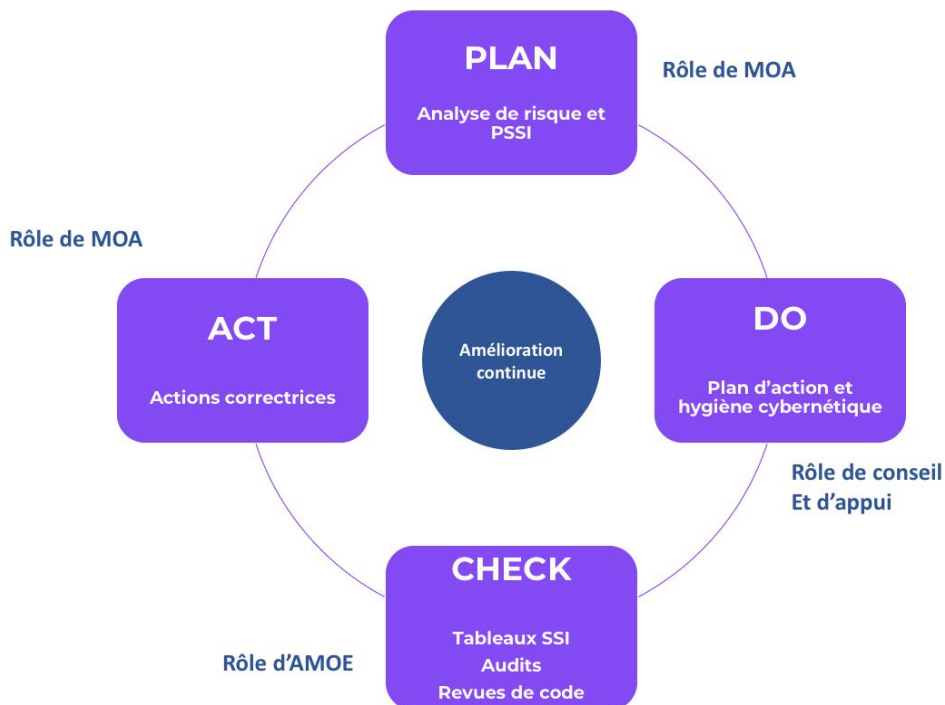
La mise en oeuvre de la PSSI se traduit par un plan d'action simple :

- **Déterminer les responsables ( Quoi, Qui ),**
- **Evaluer les ressources ( Comment ),**
- **Prioriser les objectifs**
- **Faire valider la méthodologie par la direction.**

Exemple de priorité de la première échéance :

Thématique	Objectifs	Règles
Sensibilisation du personnel	Faire connaître aux membres du laboratoire les règles élémentaires de sécurité et le comportement à adopter en cas d'incidents	1.1.4 ; 1.3.1 ; 1.3.2 ; 1.3.3 ; 1.3.4 ; 4.4.8 ;
Organisation de la SSI	Structurer et animer la fonction sécurité du laboratoire	1.1.1 ; 1.1.2 ; 1.1.4 ; 1.2.1 ;
Sécurité physique	Assurer une protection suffisante des locaux	5.1.1 ; 5.1.2 ; 5.1.5 ; 5.2.1 ;
Inventaire du SI	Cartographier le SI	4.1.1 ; 4.1.2 ; 4.1.3
Accès au SI	Assurer la mise en place de compte nominatifs à mot de passe	4.4.1 ;
	Veiller à mettre en place le verrouillage des stations en cas d'absence prolongée des utilisateurs	4.4.2 ;
Disponibilité	Mise en place d'un plan de sauvegarde	6.1.1 ; 6.1.3 ; 6.1.2 ; 6.1.5
	<u>Historisation</u>	6.2.1 ; 6.2.2 ;
Sécurité logique	Assurer la protection antivirale	4.4.3 ;
	Protection trafic Internet et logiciels malveillants	4.3.3 ; 4.1.7 ; 4.2.1
Conformité légale	Assurer une conformité minimale aux textes en vigueur	2.2.1 ; 2.1.1 ; 2.1.4

Il est fortement recommandé de suivre **le modèle PDCA** qui vise à une amélioration continue de l'ensemble des étapes clés de la PSSI par le déploiement de 4 phases :



Enfin un autre élément important qui contribue à l'amélioration continue de la PSSI : **l'hygiène cybernétique des utilisateurs**. La sensibilisation des utilisateurs du SI autour des risques, des mauvaises habitudes et des bonnes pratiques est un enjeu majeur pour l'entreprise.

### c) Mettre en place une veille en cybersécurité

Chaque jour, de nouveaux **risques** et de **nouvelles failles de sécurité** sont découverts, mettant toujours plus en péril vos données et vos systèmes. Pour assurer leur protection, il est recommandé de mettre en place une **veille efficace** pour collecter les informations et assurer une connaissance des vulnérabilités.

Cette démarche de veille permanente repose principalement sur deux piliers :

- la **supervision** : consultez les traces des serveurs et continuellement améliorer le système de supervision avec gestion d'alerte. Réagir immédiatement si ces derniers sont attaqués
- les **misés à jour** : vérifiez constamment que les composants sensibles n'ont pas besoin d'être mis à jour. Corriger ici une faille critique sur SSH, là une autre concernant HTTPD ou MySQL, etc. Informez vous des failles de sécurité grâce aux **bulletins CERT** afin de prendre les mesures nécessaires ( Applications de patch, remplacement app ou modification SI. )

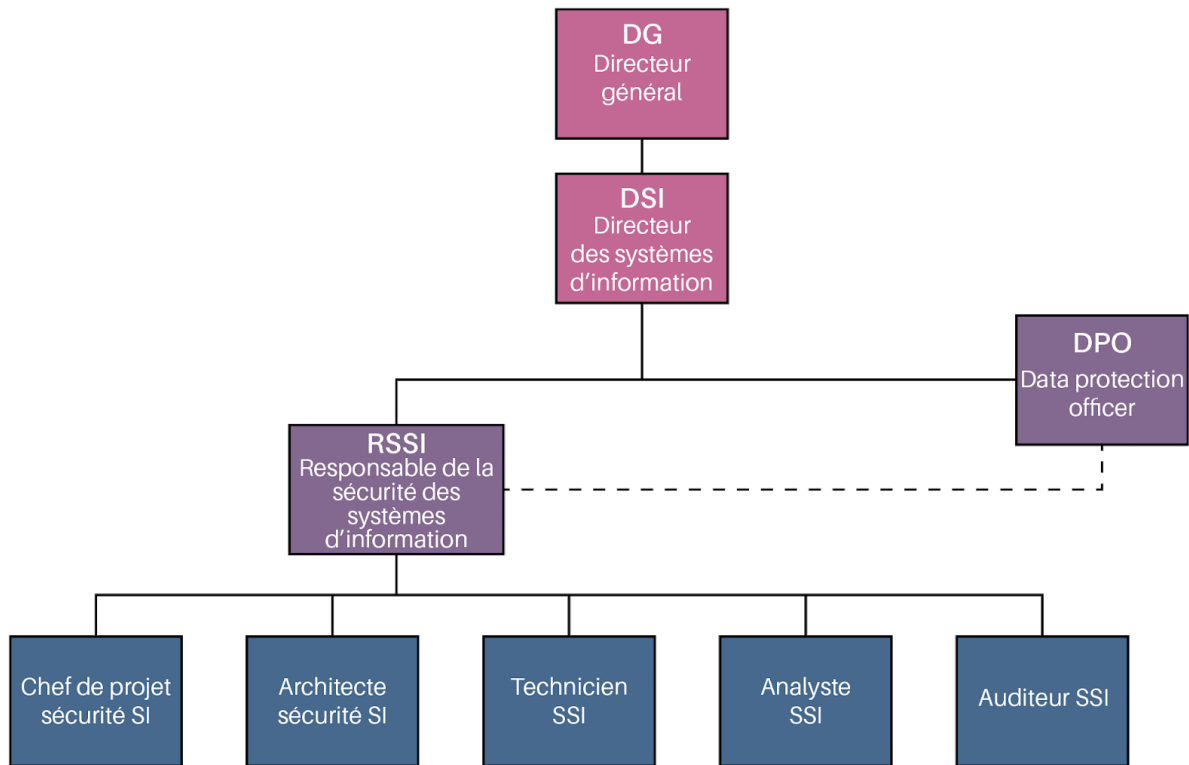
Il est également conseillé de mettre en place le même processus sur le modèle PDCA réalisé lors de la PSSI ( Préparer, développer, contrôler, ajuster ) pour une amélioration continue de la veille en cybersécurité

On pourrait prendre pour exemple la méthodologie suivante :

1. Définir d'abord les actifs via une **analyse en gestion des risques** pour comprendre ce que vous devez protéger.
2. Intégrer la veille à la **politique de sécurité des systèmes d'information (PSSI)** permettant de définir les mesures de protection à mettre en place dans un cycle continue.
3. Définir les **outils** et les **processus** que vous allez mettre en place pour **gérer les vulnérabilités**.
4. Déterminer des indicateurs permettant de mesurer l'efficacité de votre veille (indice de vulnérabilité des serveurs, nombre de services vulnérables, délai entre la publication d'un patch et son application).

Il est aussi recommandé d'**industrialiser le processus de veille au sein du PSSI** grâce à des équipes dédiées pour répondre aux tâches suivantes :

- **anticiper** les **menaces** ;
- **analyser** les **vulnérabilités** ;
- **étudier** les **attaques** ;
- **réagir** aux **incidents de sécurité** ;
- **coordonner** les **équipes** en cas de crise majeure.



#### d) Maîtriser les risques juridiques liés au numérique

Dans le cadre de ce projet, le droit est un aspect indispensable qu'il est nécessaire d'évoquer dans l'utilisation de votre application web par les utilisateurs.

Établir des conditions générales d'utilisations et les faire accepter électroniquement c'est respecter des prérogatives de sécurités ( comme le chiffrement SSL ou la robustesses des bases de données pour la protection de la vie privée ) Cela permet alors de garantir l'intégrité de l'entreprise et la confiance des clients. C'est aussi lutter plus efficacement contre la cybercriminalité mais aussi mieux protéger et informer les utilisateurs dans l'utilisation du service. On retrouvera dans les CGU :

- **La propriété intellectuel ( droit d'auteur, droit morale, droit des marques ) ;**
- **Une clause de non responsabilité pour mauvaise utilisation du service ;**
- **Une clause de responsabilité contractuel**
- **Une clause de poursuite en cas de cybercriminalité. ;**
- **Respecter des obligations en termes de données personnelles avec RGPD;**
- **Un contrat de respect dans l'utilisation du service**

Si l'offre de service en ligne fait appel à divers autres prestataires, l'entreprise assume la responsabilité concernant la bonne exécution de leur propres prestations à l'égard du client ( Par exemple l'hébergeur du site internet de l'entreprise ). Toutefois certaines clauses de non responsabilités entre en vigueur à conditions d'être mentionnées en annexe du contrat.

Dans le cas de vente de bien ou de service, il est obligatoire de rédiger un contrat claire et précis afin d'établir la responsabilité, le respect et l'engagement des deux parties.

Au delà de l'aspect informationnelle pour les protagonistes, un contrat est en droit un outil constitutionnel servant lors de poursuite juridique à la conciliation, le dédommagement ou le désengagement pour l'un des deux parties.

En matière de responsabilité, le principe (en droit français) n'est pas obligatoirement le cumul de la responsabilité délictuelle et de l'inexécution contractuelle.

*En effet il est clairement affirmé que l'on ne peut agir sur les deux fondements. Cela est, en théorie du moins, aisé à comprendre : la responsabilité délictuelle (aussi dite extracontractuelle) répare les conséquences d'une faute en dehors d'un contrat, tandis que l'inexécution contractuelle est un régime qui répare la non exécution d'une obligation contractuelle.*

Si l'utilisation du service numérique est international, il est alors important de connaître les principales méthodes du droit international dont :

- **Les règles de conflit de juridiction;**
- **Les règles de conflit de lois. ;**

Une situation juridique est internationale lorsqu'elle comporte un élément d'extranéité lequel est :

- **Un élément étranger qui a une incidence sur la détermination de la règle de droit applicable.**





**Enfin,** La CNIL est une autorité administrative indépendante (AAI), c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle est composée de 18 membres élus ou nommés et s'appuie sur des services.

Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction. Veillez donc à respecter les règles juridiques liés aux numérique.