GUIDE DE SÉCURISATION D'UN SYSTÈME LINUX

CASTEL CLÉMENT, TITOUAN LOISEL,
THOMAS LE SCORNEC

DOCUMENTATION : Sécurisation d'un système Debian

- Gestion sécurisée de comptes centralisés
  - R33 (-IRE) : Sécurisation des accès aux bases utilisateurs distantes
  - R34 (-IRE) : Séparation des comptes système et d'administrateur de l'annuaire
- Suppression des droits setuid inutiles
  - R37 (MIRE) : Exécutables avec bits setuid et setgid
  - R38 (--RE) : Exécutables setuid root
- Partitionnement fin avec droits restreints
  - R12 (-IRE) : Partitionnement type
  - R13 (--RE) : Restrictions d'accès sur le dossier /boot
- Configuration sécurisée services
  - R21 (-IRE) : Durcissement et surveillance des services soumis à des flux arbitraires
  - R22 (-IRE) : Paramétrage des sysctl système
  - R23 (-IRE) : Paramétrage des sysctl système
- Règles iptables pour trafic entrant

Niveau de sécurité : RENFORCÉ

- Écriture de scripts d'audit spécialisés
  - R35 (--RE) : Valeur de umask
  - R36(-IRE) : Droits d'accès aux fichiers de contenu sensible
  - Optionnel : Fichiers sans utilisateur ou groupe propriétaire
  - R39 (-IRE) : Répertoires temporaires dédiés aux comptes
  - R40 (-IRE) : Sticky bit et droits d'accès en écriture
  - R41 (-IRE) : Sécurisation des accès pour les sockets et pipes nommées
- Suppression des programmes innutiles
  - R1 (MIRE) : Minimisation des services installés
  - R2 (MIRE) : Minimisation de la configuration
- Blocage du chargement dynamique de modules
  - R24 (--RE) : Désactivation du chargement des modules noyau
  - R25 (--RE) : Configuration sysctl du module Yama
- Configuration sécurisée système
  - R22 (-IRE) : Paramétrage des sysctl système
  - R23 (-IRE) : Paramétrage des sysctl système
- Journalisation de l'activité par auditd
  - R50 (--RE) : Journalisation de l'activité par auditd
- Règles iptables pour trafic local et sortant

Niveau de sécurité : ÉLEVÉ

- Confinement par AppArmor
  - R65 (---E) : Activation des profils de sécurité AppArmor
  - Optionnel : création d'un nouveau profil

ALLER PLUS LOIN : BLINDAGE LYNIS

- Couldn't find 2 responsive nameservers [NETW-2705]
- This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
- Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]
- Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
- Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
- Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
- Consider hardening system services [BOOT-5264]
- If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
- Configure maximum password age in /etc/login.defs [AUTH-9286]
- Configure minimum password age in /etc/login.defs [AUTH-9286]
- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
- Copy /etc/fail2ban/jail.conf to jail.local to prevent it being changed by updates. [DEB-0880]
- Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
- Determine if protocol 'dccp' is really needed on this system [NETW-3200]
- Determine if protocol 'sctp' is really needed on this system [NETW-3200]
- Determine if protocol 'rds' is really needed on this system [NETW-3200]
- Determine if protocol 'tipc' is really needed on this system [NETW-3200]
- Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
- Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

Nos Scans de sécurité

Scan	Commentaire
Fin Installation	Score = 66 % ; Warnings : 1 ; Suggestions : 40
Fin Étape 1	Score = 67 % ; Warnings : 1 ; Suggestions : 40
Fin Étape 2	Score = 69 % ; Warnings : 1 ; Suggestions : 37
Fin Étape 4	Score = 70 % ; Warnings : 1 ; Suggestions : 36
Fin Projet (avec blindage Lynis)	**Score = 84 % ; Warnings : 0 ; Suggestions : 12**

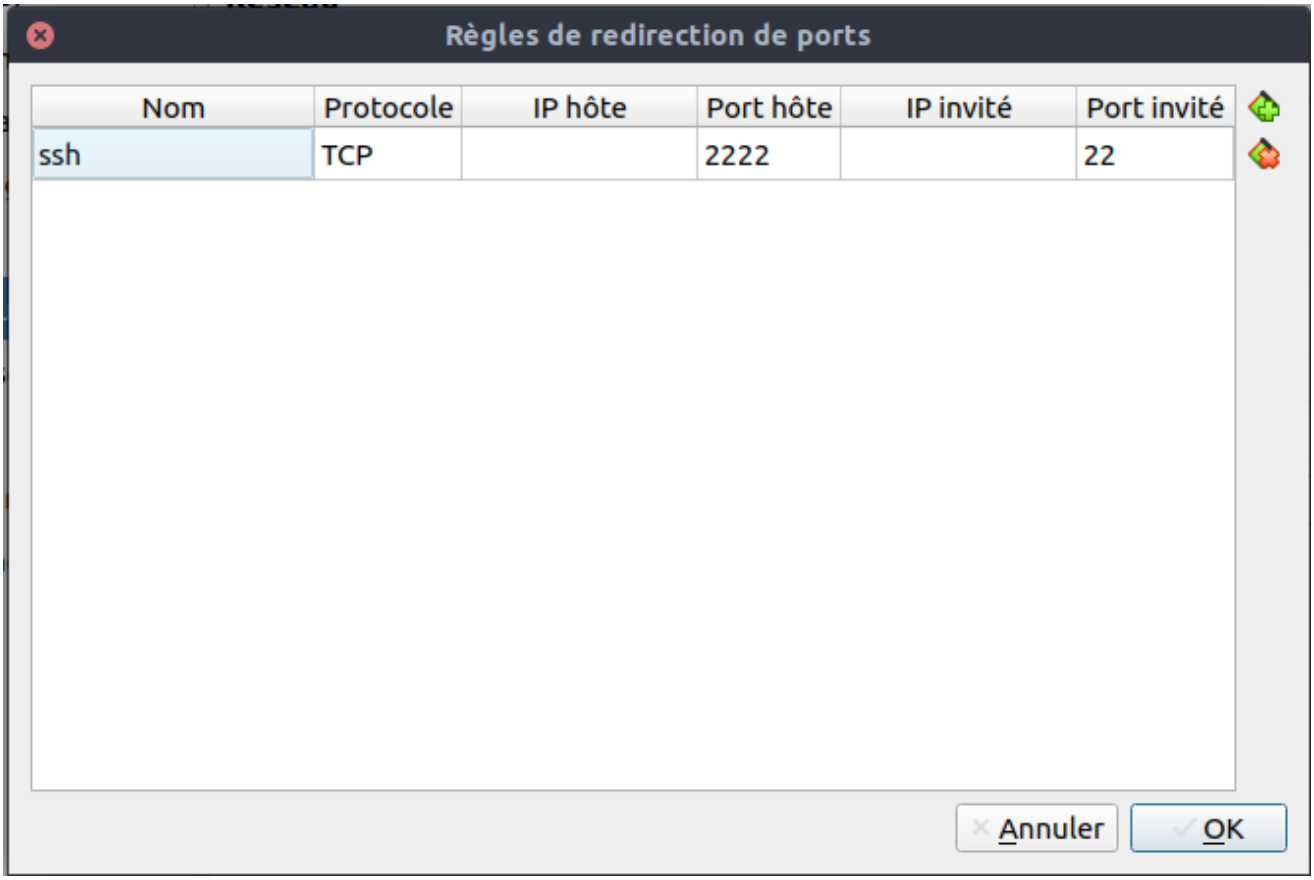
Installation

- Installation non graphique
- Choix de LVM chiffré
- Mot de passe solide
  - Pour root (généré à partir de Dashlane) : `O6@t&W!PCbPHR9SgfGJ5Q5dzhk$BarO#0@#Fy2H4`
  - Pour l'utilisateur "clement" : `n!XbtjgKnn@nfktoZq5fw9Gj?U8CxGQ5ymLj2WRO`
- Une passphrase solide : `H5iCcjRNu2itqAI2&9amsk!1xRdhzc&FX#Sr1?1r`

Connexion ssh

Dans Virtualbox :

Configuration -> Réseau ->
"Mode d'accès réseau" : NAT
Avancé -> Redirection de ports ->
Nouvelle règle (ssh | TCP | | 2222 | | 22)



Dans un terminal sur la machine hote

```
ssh -p 2222 clement@127.0.0.1
```

puis `su root`

Premier tests de sécurité

Debsecan

Debsecan sert à analyser les packages installés sur la machine et à mettre en évidence ceux qui comportent des vulnérabilités.
La commande suivante sert à effectuer un scan :

```
debsecan --suite $(lsb_release --codename --short) --only-fixed --format detail
```

La commande ne devrais rien retourner, sinon il faut faire les mises à jour.
Rappel : `apt update && apt upgrade`

Lynis

Pour effectuer un premier scan Lynis, il faut dans un premier temps se placer dans le répertoire où se situe Lynis puis effectuer la commande suivante :

```
./lynis audit system
```

Il peut être utile de convertir le rapport que fournis Lynis en Html :

```
/usr/sbin/lynis audit system | ansi2html -l > report.html
```

Pour rappel, la commande suivante permet de copier un un fichier via le ssh :

```
scp -P2222 username@127.0.0.1:report.html report.html
```

Niveaux de sécurité système

Minimal

- Application systématique des correctifs
- Limitation des services réseau lancés
- Mots de passes complexes
- Configuration robuste de PAM

Intermédiaire

- Règles iptables pour trafic entrant
- Configuration sécurisée services
- Partitionnement fin avec droits restreints
- Suppression des droits setuid inutiles
- Gestion sécurisée de comptes centralisés
- Journalisation et déport des journaux
- Confinement de droits par sudo

Renforcé

- Règles iptables pour trafic local et sortant
- Journalisation de l'activité par auditd
- Configuration sécurisée système
- Blocage du chargement dynamique de module
- Suppressions des programmes inutiles
- chroot systématique de tous les services
- Écriture de scripts d'audit spécialisés

Élevé

- Utilisation du RBAC de SELinux
- Confinement par AppArmor

Niveau de sécurité : MINIMAL

Application systématique des correctifs

L'objectif de cette partie est de sécuriser le système en ayant tout le temps les dernières mises à jour des paquets. Cela permet d'éviter les failles connues.

R7 (--RE) Journalisation de l'activité des services & R8 (MIRE) Mises à jour régulières [Méthode 1]

On commence par installer cron. Cet outils permet d'exécuter automatiquement des scripts à interval donnés.

```
apt install cron-apt
```

Il est ensuite important de télécharger et installer uniquement les paquets de sécurité : pour cela il faut créer ou éditer le fichier `/etc/cron-apt/action.d/5-security`
Note : On peut utiliser vi par exemple : `vi /etc/cron-apt/action.d/5-security`

On y rajoute ensuite la ligne suivante : `upgrade -y -o APT::Get::Show-Upgraded=true`

Il faut ensuite éditer le fichier `/etc/apt/sources.list` en commentant (ajouter un '#' en début de ligne) les lignes contenant "security" dans l'URL et copier ces lignes. On crée ou édite le fichier `/etc/apt/sources.list.d/security.list` et on y colle les lignes copiées en les décommentant.

Pour finir, éditer le fichier `/etc/cron-apt/action.d/5-security` et y ajouter la ligne :

```
OPTIONS="-o quiet=1 -o APT::Get::List-Cleanup=false -o
Dir::Etc::SourceList=/etc/apt/sources.list.d/security.list -o
Dir::Etc::SourceParts=\"/dev/null\""
```

Cette ligne indique au paquet cron-apt de ne mettre à jour systématiquement que les paquets provenants des sources dans security.list (fichier créé précedemment).

R7 (--RE) Journalisation de l'activité des services & R8 (MIRE) Mises à jour régulières [Méthode 2]

Pour cette méthode, nous utiliserons `unattended-upgrades`. Il faut commencer par l'installer avec la commande suivante :

```
apt-get install unattended-upgrades apt-listchanges
```

On édite ensuite le fichier `/etc/apt/apt.conf.d/50unattended-upgrades` de la façon suivante pour choisir quels paquets doivent êtres upgrade (décommenter les lignes souhaitées):

```
Unattended-Upgrade::Origins-Pattern {
    // ...
};
```

Il faut au moins décommenter la ligne suivante :

```
Unattended-Upgrade::Mail "root";
```

Pour effectuer des appels automatiques à ce fichier on modifie le fichier `/etc/apt/apt.conf.d/20auto-upgrades` pour ajouter les lignes suivantes :

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Mais il faut précédemment créer le fichier `20auto-upgrades` avec la commande `dpkg-reconfigure -plow unattended-upgrades`.

Limitation des services réseau lancés

R42 (MIRE) Services et démons résidents en mémoire

Pour lister les services on utilise la commande : `/usr/sbin/service --status-all`
ou sinon : `systemctl list-units --type=service`

Pour désactiver un service : `systemctl disable <service_name>`

Note : ayant une installation minimale il n'y a pas (ou peu) de services à désactiver. La plupart sont essentiels au bon fonctionnement de Debian

Mots de passe complexe

R18 (MIRE) Robustesse du mot de passe administrateur

Il est nécessaire d'avoir des mots de passe forts pour se connecter à la machine. Pour générer des mots de passe dans Dashlane :

- Ouvrir Dashlane, aller dans la partie `Générateur`
    - Mettre la longueur à 40

- S'assurer que "Lettres"/"Chiffres"/"Symboles"/"Caractères semblables" sont cochés
- Copier

Voici plusieurs exemples des mots de passe/passphrase générés dans le cadre de ce projet :

- root : `O6@t&W!PCbPHR9SgfGJ5Q5dzhk$BarO#0@#Fy2H4`
- clement : `n!XbtjgKnn@nfktoZq5fw9Gj?U8CxGQ5ymLj2WRO`
- passphrase : `H5iCcjRNu2itqAI2&9amsk!1xRdhzc&FX#Sr1?1r`

⚠️ Il faudra faire très attention à ne pas perdre ces mots de passe.

Note : Chaque administrateur doit posséder un compte dédié (local ou distant), et ne pas utiliser le compte root comme compte d'accès pour l'administration du système. Les opérations de changement de privilèges devront reposer sur des exécutables permettant de surveiller les activités réalisées (par exemple sudo).

Configuration robuste de PAM

R30 (MIRE) Applications utilisant PAM

Le nombre d'applications utilisant PAM doit être réduit au strict nécessaire afin de limiter l'exposition d'éléments d'authentification sensibles.

R31 (-IRE) Sécurisation des services réseau d'authentification PAM

Quand l'authentification se déroule au travers d'un service distant (réseau), le protocole d'authentification utilisé par PAM doit être sécurisé (chiffrement du flux, authentification du serveur distant, mécanismes d'anti-rejeu, etc.).

Ensuite, il faut bloquer un compte pendant 5 mintues après 3 tentatives de mot de passe échoué. Pour cela, on modifie le fichier login :`vim /etc/pam.d/login`
Et ajouter les lignes :

```
# Block account for 5 minutes (300 seconds) after 3 password fails
auth    required    pam_tally.so deny=3 lock_time=300
```

Et faire de même avec le fichier `/etc/pam.d/sshd`

Pour changer les règles de complexité des mots de passe, il faut éditer le fichier `/etc/pam.d/passwd` : `vim /etc/pam.d/passwd`
Et ajouter ces lignes :

```
password    required    pam_cracklib.so minlen=12 minclass=3                    \
                                                  dcredit=0 ucredit=0 lcredit=0     \
                                                  ocredit=0 maxrepeat=1             \
                                                  maxsequence=1 gecoscheck          \
                                                  reject_username enforce_for_root
```

R32 (MIRE) Protection des mots de passe stockés

Tout mot de passe doit être protégé par des mécanismes cryptographiques évitant
de les exposer en clair à un attaquant récupérant leur base.
Pour protection des mots de passe stockés : `vim /etc/pam.d/common-password`
Et éditer cette ligne : `password [success=1 default=ignore] pam_unix.so obscure sha512 rounds=65536`

De plus, il faut modifier le fichier `/etc/login.defs` à la ligne 278 :

```
ENCRYPT_METHOD  SHA512
SHA_CRYPT_MIN_ROUNDS 65536
```

Dans `/etc/pam.d/common-password` on ajoute :

```
password required pam_unix.so obscure sha512 rounds=65536
```

⚠️ **Les méthodes suivantes peuvent vous enfermer dehors** ⚠️
Interdiction de connection ssh à certains utilisateurs via le fichier `/etc/pam.d/sshd` :

```
auth    required    pam_listfiles.so    onerr=succeed    item=user    sense=deny
file=/etc/ssh/deniedusers
```

Et dans le fichier `/etc/ssh/denieduser` on pourra mettre tous les noms d'utilisateur qui ne doivent pas être accessible par ssh.
Par exemple si on veut interdire l'accès à root :
`vim /etc/ssh/deniedusers`:

```
root
```

Et si fichier /etc/ssh/deniedusers vient d'être créé, alors `chmod 600`

Lynis : libpam-tmpdir

Pour installer libpam-tmpdir (recommandé par Lynis pour compléter la robustesse de PAM) on exécute la commande suivante :

```
apt install libpam-tmpdir
```

Warning Lynis : Couldn't find 2 responsive nameservers [NETW-2705]

Éditer le fichier contenant les adresses des serveurs de résolution DNS : `vim /etc/resolv.conf`
Ajouter une nouvelle ligne avec l'adresse d'un second serveur de résolution DNS. Par exemple pour les serveurs de Cloudflare : `nameserver 1.1.1.1`

Niveau de sécurité : INTERMÉDIAIRE

Confinement de droits par sudo

R57 (-IRE) Groupe dédié à l'usage de sudo

Voici les droits par défaut du fichier /usr/bin/sudo :

```
-rwsr-xr-x 1 root root 179K févr. 27  2021 /usr/bin/sudo
```

On va donc créer un groupe 'sudogrp' pour que seuls les éléments de ce groupe puisse utiliser sudo :

```
sudo groupadd sudogrp
```

Restreindre l'accès à sudo aux seuls membres du groupe (changement propriétaire du fichier : chown) reviens à effectuer les manipulations suivantes :
+ changer des permissions (chmod, pour permettre setuid (sticky bit s)):
root@debian:~# chown root:sudogrp /usr/bin/sudo
root@debian:~# chmod 4750 /usr/bin/sudo
root@debian:~# ls -lah /usr/bin/sudo
-rwsr-x--- 1 root sudogrp 179K févr. 27 2021 /usr/bin/sudo

Vérification avec 'clement' qui execute 'sudo', et n'appartient pas à 'sudogrp':

```
clement@debian:~$ sudo
bash: /usr/bin/sudo: Permission denied
```

Ajouter l'utilisateur 'clement' à sudogrp :

```
root@debian:~# sudo usermod -a -G sudogrp clement
```

Vérification que 'clement' appartient à 'sudogrp' et peut executer `sudo` :

```
clement@debian:~$ groups
clement cdrom floppy audio dip video plugdev netdev bluetooth sudogrp
```

Test avec la commande `sudo` :

```
clement@debian:/root$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host]
[-p prompt] [-R directory] [-T timeout] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host]
[-p prompt] [-R directory] [-T timeout] [-u user]
            file ...
```

Note: Pour retirer l'utilisateur 'clement' du groupe 'sudogrp' on exécute la commande suivante :

```
gpasswd -d clement sudogrp
```

R58 (-IRE) : Directives de configuration sudo

Directives nécessaires dans `/etc/sudoers` :

```
Defaults    noexec, requiretty, use_pty, umask=0027
Defaults    ignore_dot, env_reset, passwd_timeout=1
```

Explication :

noexec	**appliquer le tag NOEXEC par defaut sur les commandes**
requiretty	imposer à l'utilisateur d'avoir un tty de login
use_pty	utiliser un pseudo-tty lorsqu'une commande est exécutée
umask=0027	forcer umask à un masque plus restrictif
ignore_dot	ignorer le '.' dans $PATH
env_reset	réinitialiser les variables d'environnement
passwd_timeout=1	allouer 1 minute pour entrer son mot de passe

R59 (MIRE) : Authentification des utilisateurs exécutant sudo

Par défaut à l'installation de sudo : le système demande que l'utilisateur soit authentifié avant de pouvoir exécuter une commande en tant que `sudo`.

R60 (-IRE) : Privilèges des utilisateurs cibles pour une commande sudo

Pour toute commande, il est préférable que des droits d'utilisateur simple et minimaux lui soient appliqués afin d'éviter une escalade de privilège.

Pour rappel:

- `r` est le droit de **lecture** (read)
- `w` est le droit d'**écriture** (write)
- `x` est le droit **d'exécution** (execute)

R61 (--RE) : Limitation du nombre de commandes nécessitant l'option EXEC

Les commandes nécessitant l'exécution de sous-processus (tag EXEC) doivent être explicitement listées et réduites autant que possible au strict minimum.

Pour cela, une solution pourrait être de lister dans le fichier `/ect/sudoers` toutes les commande qu'un utilisateur ou groupe d'utilisateurs peut exécuter en y listant seul les commandes souhaitées.

Note : Pour modifier le fichier `sudoers` il faut utiliser la commande `sudo visudo`.

R62 (-IRE) : Du bon usage de la négation dans une spécification sudo

Le principe de liste noire est inefficace car cela est facilement contournable (copie puis renommage de l'executable). On y préferera les listes blanches où l'on donne accès au stricte nécessaire et où le controle est plus fin sur les permissions/droits de chaque utilisateur/groupe.

R63 (-IRE) : Arguments explicites dans les spécifications sudo

Dans le ficher de configuration de `sudo` (`/etc/sudoers`) toutes les commandes doivent préciser strictement les arguments autorisés à être utilisés pour un utilisateur donné. L'utilisation de * doit être réduit au strict minimum (il est préférable de ne pas l'utiliser). En fin, l'abscence d'argument doit être spécifié par la présence d'une chaine de caractères vide (`""`).

Note : Pour modifier le fichier `sudoers` il faut utiliser la commande `sudo visudo`.

R64 (-IRE) : Du bon usage de sudoedit

Les éditeurs de fichiers modernes sont fonctionnellement riches et certains permettent d'exécuter des fichiers (notamment des scripts bash) depuis leur interface. Le danger est d'éditer un fichier en utilisant sudo (par exemple : `sudo vim /usr/bin/fichierXYZ.sh`) puis executer ce fichier depuis l'éditeur (dans vim : `:make` pour lancer un Makefile du répertoire du fichier en cours d'édition directement depuis l'éditeur).
Pour éviter cela, il est préférable (voire obligatoire) d'utiliser sudoedit (copie de nano mais avec une sécurité renforcée) pour éditer les fichiers où l'on a besoin d'utiliser 'sudo'.

Journalisation et déport des journaux

R43 (-IRE) : Durcissement et configuration du service syslog

Reprise des éléments de recommandation de l'ANSSI à propos de la "journalisation" :

1. Pré-requis :
    1. Fonctionnalité de journalisation
       `syslog` est installé par défaut sur tous les systèmes Debian. Ce fonctionnement natif permet aux utilisateurs et administrateurs d'être en sécurité en cas de problème car il y aura une trace des actions en cas de problème.

2. Horodatage des évènements
   Tous les évènements sont horodatés pour faciliter le suivi.
   Voici un exemple de la trace conservée lors d'une connexion réussie au compte 'clement' par ssh :

   ```
   Sep 29 10:08:50 debian systemd[1]: Started Session 12 of user clement.
   Sep 29 10:08:50 debian systemd[1]: session-12.scope: Succeeded.
   ```

   On y voit le jour, l'heure, le nom de la machine (debian) et le nom du processus (systemd) avec un détail de l'évènement.

3. Synchronisation des horloges
   `syslog` utilise l'heure locale de la machine.
   Il est possible de spécifier un fuseau horaire différent si l'on utilise syslog-ng (une évolution plus moderne de syslog, installé nativement sur Debian jusqu'en 2014) ou rsyslog (remplacant de syslog-ng depuis 2014). Cela est particulièrement utile dans le cas d'une entreprise ayant des serveurs répartis dans le monde.
   Pour plus d'informations à propos du change de fuseau horaire sur rsyslog : https://www.rsyslog.com/doc/master/configuration/timezone.html

4. Dimensionnement

   1. Espace disque
      La taille maximale d'un évènement est de 8K. Il est possible de modifier la variable `$MaxMessageSize` dans le fichier de configuration `/etc/rsyslog.conf`
      La taille totale des logs est limitée à 100 MB. Qu'il est aussi possible de modifier dans le fichier de configuration.

      (Anecdote: Ubuntu est connu dans ses dernières versions pour ne pas toujours limiter la taille du fichier /var/log/syslog. Il m'est arrivé plusieurs fois que mon système ralentisse brutalement car le fichier occupait tout l'espace disque. Et je me retrouvais avec un fichier de log de plus de 80 GB).

   2. Résistance à la charge
      Si l'on regarde la priorité du processus de log il est à 20. Il a donc une priorité aussi importante que tout autre processus lancé par l'utilisateur.
      En cas de charge anormale de la machine, il se comportera comme les autres processus. Pour éviter de surcharger le système, il garde les messages en attente dans la mémoire.

2. Recommandations d'architecture & conception

   1. Résilience du système

      1. Exportation des journaux
         Les journaux ne sont pas automatiquement exportés vers une autre machine. Mais il est possible de les envoyer sur un autre serveur de log nativement avec rsyslog (plus d'infos ici : https://stackoverflow.com/questions/35264438/how-to-forward-specific-log-file-to-a-remote-rsyslog-server)
      2. Centralisation des journaux
         Les logs sont centralisés dans un fichier : `/var/log/syslog`
         Ce fichier peut ensuite être envoyé vers un serveur de log comme expliqué ci-dessus. Ce serveur est ensuite en mesure de centraliser les logs en provenance de plusieurs machines.

   2. Protection des données échangées

      1. Modes de transfert
         Les logs sont envoyés sur le port TCP 514 en temps réel.
         Il est possible de configurer rsyslog pour envoyer les logs tous les X temps ou tous les Y évènements.
      2. Prétraitement des journaux
         Un prétraitement des journaux peut être effectué mais si rien n'est fait pour, alors c'est une copie exacte des fichiers qui est envoyé.
      3. Fiabilisation du transfert des journaux
         Le protocole TPC est utilisé.
      4. Sécurisation du transfert des journaux
         Il est possible (et fortement recommandé) d'envoyer les fichiers de logs en utilisant une méthode de chiffrement asymétrique (si la méthode est trop lente pour le volume de données à envoyer alors on préférera un chiffrement

hybride (asymétrique+symétrique)).
Pour en savoir plus sur la mise en place des clés et la procédure d'envoi : https://www.thegeekdiary.com/how-to-configure-rsyslog-server-to-accept-logs-via-ssl-tls/
Sinon il est possible de créer un serveur Apache pour réceptionner les logs. Mais c'est une solution à proscrire car les logs transitent en clair.

5. Bande passante
   (dépend du réseau de l'entreprise)
6. Utilisation du réseau d'administration
   Il est possible d'envoyer des fichiers de logs sur un réseau local sans passer par internet. Et ainsi éviter d'exposer les fichiers à l'extérieur.

3. Stockage

   1. Partition séparée
      Il est possible d'utiliser une partition séparée pour le stockage des logs. C'est d'ailleurs conseillé au moment de l'installation.
   2. Arborescence
      Les fichiers de logs sont séparés dans `/var/log`. Voici l'exemple des fichiers créés sur le serveur Debian :

      ```
      alternatives.log  dpkg.log   lynis.log             runit
      apt         exim4      lynis-report.dat         syslog
      auth.log    faillog    messages             user.log
      btmp        installer  popularity-contest       vboxadd-install.log
      cron-apt    journal    popularity-contest.0     vboxadd-setup.log
      daemon.log      kern.log   popularity-contest.1.gz  vboxadd-setup.log.1
      debug       lastlog    private              wtmp
      ```

   3. Rotation

      Rsyslog gère par défaut la rotation des logs (pour en savoir plus : https://www.rsyslog.com/doc/master/tutorials/log_rotation_fix_size.html#).
   4. Archivage

      Il est imaginable qu'une entreprise veuille stocker une copie de ses fichiers de logs sur un support de stockage permettant l'archivage en cas de nécessité dans le futur.
   5. Protection des journaux

      Les droits d'accès doivent être définis par l'administration. Pour, par exemple, interdire à l'utilisateur lambda d'avoir accès aux logs système.

4. Consultation

   1. Choix d'un outil
      Il est possible d'utiliser la commande `tail` pour visualiser un fichier de log. Cette commande est très flexible et permet aussi bien de voir les X dernières lignes d'un fichier, ou de suivre en direct son évolution.

      Sinon il existe aussi des outils proposant une interface graphique : Glogg, Graylog, GoAccess
   2. Définition des roles
      Comme dit précédemment, il convient à l'administrateur de définir qui a accès à quels logs.

5. Supervision de l'espace disque
   Il convient à l'administrateur de surveiller la place qu'occupent les logs sur le serveur et s'assurer que la partition n'est jamais pleine.

R44 (-IRE) : Cloisonnement du service syslog par chroot

Quand cela est possible, il faut cloissonner le service `syslog` grâce à un chroot. Pour cela nous allons dans un premier temps créer le nouvel espace (en donnant par exemple le nom J : `J=$HOME/location`) dans lequel nous allons créer le dossier `syslog`. Nous copier à l'aide de la commande `cp` le service `syslog` dans son nouvel espace. Il faut ensuite déterminer les différentes dépendances de `syslog` grâce à la commande `ldd`. Il faut ensuite copier chaque librairie dans l'espace qui sera chroot en respectant bien l'arboraissance donnée avec la commande `ldd`. Et enfin il ne reste plus qu'a utiliser la commande `chroot <espace créeé>` pour finaliser le chroot de `syslog`.

R45 (---E) : Cloisonnement du service syslog par conteneur

Le service syslog doit être isolé du reste du système dans un conteneur dédié.

R46 (-IRE) : Journaux d'activité de service

Afin d'être en mesure de retrouver un coupable dans le cas d'un problème, ou en général pouvoir trouver qu'elle est la source d'un bug, il est important d'avoir des journaux d'activité (logs) séparés dans des fichiers indépendants pour chaque service.
Un fichier de log d'un service ne doit pas être manipulable par un autre service que celui dont il contient la journalisation.
Un fichier de log ne doit pas être effacable ou altéré en cas de compromission.

R47 (-IRE) : Partition dédiée pour les journaux

Les logs sont une partie critique de tous systèmes. Il faut s'assurer qu'ils ne peuvent pas être perdus. Pour cette raison, il faut toujours que les logs soient sur une partition dédiée. De cette manière, si un processus vient à remplir l'espace disque d'autres partitions (par exemple `/home/clement/`), la partition des logs aura toujours de l'espace pour continuer à journaliser le processus. Ainsi, le développeur pourra lire les journaux pour comprendre ce qu'il s'est passé et éviter que cela se reproduise à l'avenir.

Gestion sécurisée de comptes centralisés

R33 (-IRE) : Sécurisation des accès aux bases utilisateurs distantes

Dans le cas où les bases utilisateurs sont stockées sur un service réseau distant, NSS doit être en mesure d'établir une liaison sécurisée (chiffrement asymétrique de préférence) en authentifiant au minimum le serveur.

R34 (-IRE) : Séparation des comptes système et d'administrateur de l'annuaire

Les comptes utilisés sur un système d'exploitation doivent être différents des comptes utilisés pour administrer l'annuaire NSS.
Les comptes administrateurs d'annuaire ne doivent pas pouvoir faire des requêtes d'énumération de comptes par NSS.

Suppression des droits setuid inutiles

R37 (MIRE) : Exécutables avec bits setuid et setgid

Le bit setuid est présent sur des fichiers ayant les droits d'execution. Ce bit signifie que lorsque le fichier est executé, il prend les permissions de l'utilisateur qui a créé le fichier et non ceux de l'utilisateur qui lance le fichier.
Le bit de setgid fonctionne sur le même principe, avec le gid (group id).

Pour identifier la présence de ce bit, on peut faire `ls -l <<mon_fichier>>`. Ce qui donnera un résultat comme celui ci :

```
clement@debian:/tmp$ ls -l setuid.sh
-rwSr--r-- 1 clement clement 0 oct.   5 15:05 setuid.sh
```

On peut voir dans les droits utilisateur 'rwS', le 'S' est majuscule car les droits d'execution n'ont pas été donnés. Si on l'ajoute alors le 's' devient minuscule.

Pour ajouter le droit setgid, on utilise la commande `chmod g+s <<mon_fichier>>`

Voici ce qui est affiché quand on ajoute à un fichier les droits d'execution (utilisateur et groupe) et les droits de setuid et setgid:

```
clement@debian:/tmp$ ls -l setuid.sh
-rwsr-sr-- 1 clement clement 0 oct.   5 15:05 setuid.sh
```

Vous comprenez les dangers et la portée de l'utilisation de ces droits. Ils permettent de faire des élévations de privilège facilement en usurpant les droits d'autres utilisateurs. L'élévation de privilège va de changer le comportement du programme à usurper l'identité de root.

Il faut donc utiliser ces droits avec précaution et les accorder uniquement quand c'est nécessaire et quand on sait ce que l'on fait.

R38 (--RE) : Exécutables setuid root

Comme expliqué ci-dessus, il faut limiter les fichiers avec les droits setuid et setgid. Une bonne pratique est de n'autoriser ces droits que pour les fichiers qui sont possédés (et executables) par root ou le groupe sudo (qui pourront donc être limités par l'accès au groupe sudo et l'utilisation de la commande su/sudo).

Il est recommandé de faire un scan des fichiers avec ces droits après chaque mise à jour. On peut même le faire après chaque installation de programme pour être vraiment prévoyant.

Pour lister les fichiers sur le système avec les droits setuid/setgid, on peut utiliser :`find / -type f -perm /6000 -ls 2>/dev/null`
Et voici un exemple de retour de la commande :

```
root@debian:~# find / -type f -perm /6000 -ls 2>/dev/null
       22      0 -rwsr-sr--   1 clement  clement         0 oct.  5 15:05 /tmp/setuid.sh
   260123      0 -rwsr-xr-x   1 root     root            0 juil. 28 18:26
/opt/VBoxGuestAdditions-6.1.26/bin/VBoxDRMClient
     7639    472 -rwsr-xr-x   1 root     root       481608 mars 13  2021
/usr/lib/openssh/ssh-keysign
   652635     52 -rwsr-xr--   1 root     messagebus    51336 févr. 21  2021
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   650330     52 -rwsr-xr-x   1 root     root          52880 févr.  7  2020
/usr/bin/chsh
   653810     44 -rwsr-xr-x   1 root     root          44632 févr.  7  2020
/usr/bin/newgrp
   660400    348 -rwxr-sr-x   1 root     ssh          354440 mars 13  2021 /usr/bin/ssh-
agent
   650332     88 -rwsr-xr-x   1 root     root          88304 févr.  7  2020
/usr/bin/gpasswd
   653959     72 -rwsr-xr-x   1 root     root          71912 juil. 28 21:09 /usr/bin/su
   652662     24 -rwxr-sr-x   1 root     tty           22760 juil. 28 21:09
/usr/bin/write.ul
   650333     64 -rwsr-xr-x   1 root     root          63960 févr.  7  2020
/usr/bin/passwd
   650329     60 -rwsr-xr-x   1 root     root          58416 févr.  7  2020
/usr/bin/chfn
   662985     16 -rwxr-sr-x   1 root     root          15208 nov. 19  2020
/usr/bin/dotlock.mailutils
   654248     56 -rwsr-xr-x   1 root     root          55528 juil. 28 21:09
/usr/bin/mount
   663252     36 -rwsr-xr-x   1 root     root          35048 juin 20 15:45
/usr/bin/fusermount3
   660046     24 -rwxr-sr-x   1 root     mail          23040 févr.  4  2021
/usr/bin/dotlockfile
   654250     36 -rwsr-xr-x   1 root     root          35040 juil. 28 21:09
/usr/bin/umount
   650328     80 -rwxr-sr-x   1 root     shadow        80256 févr.  7  2020
/usr/bin/chage
   663335    180 -rwsr-x---   1 root     sudogrp      182600 févr. 27  2021
/usr/bin/sudo
   651739     36 -rwxr-sr-x   1 root     tty           35048 juil. 28 21:09
/usr/bin/wall
   650331     32 -rwxr-sr-x   1 root     shadow        31160 févr.  7  2020
/usr/bin/expiry
   655677     44 -rwxr-sr-x   1 root     crontab       43568 févr. 22  2021
/usr/bin/crontab
   650313     40 -rwxr-sr-x   1 root     shadow        38912 juil.  9 18:55
/usr/sbin/unix_chkpwd
   662693   1332 -rwsr-xr-x   1 root     root        1360680 juil. 13 18:04
/usr/sbin/exim4
   654374     12 -rwsr-xr-x   1 root     root          10600 mars  8  2012
/usr/sbin/pam-tmpdir-helper
```

Analyse : à première vue, notre système respecte la première règle : limiter à root les fichiers setuid et setgid.

Il y a ensuite un ensemble de recommandations pour des fichiers spécifiques :

Éxecutable	**Commentaire**
/bin/mount	À désactiver, sauf si absolument nécessaire pour les utilisateurs.
/bin/netreport	À désactiver.

Éxecutable	Commentaire
/bin/ping6	(IPv6) Idem ping.
/bin/ping	(IPv4) Retirer droit setuid, sauf si un programme le requiert pour du monitoring.
/bin/su	Changement d’utilisateur. Ne pas désactiver.
/bin/umount	À désactiver, sauf si absolument nécessaire pour les utilisateurs.
/sbin/mount.nfs4	À désactiver si NFSv4 est inutilisé.
/sbin/mount.nfs	À désactiver si NFSv2/3 est inutilisé.
/sbin/umount.nfs4	À désactiver si NFSv4 est inutilisé.
/sbin/umount.nfs	À désactiver si NFSv2/3 est inutilisé.
/sbin/unix_chkpwd	Permet de vérifier le mot de passe utilisateur pour des programmes non root. À désactiver si inutilisé.
/usr/bin/at	À désactiver si atd n’est pas utilisé.
/usr/bin/chage	À désactiver.
/usr/bin/chfn	À désactiver.
/usr/bin/chsh	À désactiver.
/usr/bin/crontab	À désactiver si cron n’est pas requis.
/usr/bin/fusermount	À désactiver sauf si des utilisateurs doivent monter des partitions FUSE.
/usr/bin/gpasswd	À désactiver si pas d’authentification de groupe.
/usr/bin/locate	À désactiver. Remplacer par mlocate et slocate.
/usr/bin/mail	À désactiver. Utiliser un mailer local comme ssmtp.
/usr/bin/newgrp	À désactiver si pas d’authentification de groupe
/usr/bin/passwd	À désactiver, sauf si des utilisateurs non root doivent pouvoir changer leur mot de passe.
/usr/bin/pkexec	À désactiver si PolicyKit n’est pas utilisé.
/usr/bin/procmail	À désactiver sauf si procmail est requis.
/usr/bin/rcp	Obsolète. À désactiver.
/usr/bin/rlogin	Obsolète. À désactiver.
/usr/bin/rsh	Obsolète. À désactiver.
/usr/bin/screen	À désactiver.
/usr/bin/sudo	Changement d’utilisateur. Ne pas désactiver.
/usr/bin/sudoedit	Idem sudo.

Éxecutable	Commentaire
/usr/bin/wall	À désactiver.
/usr/bin/X	À désactiver sauf si le serveur X est requis.
/usr/lib/dbus-1.0/dbusdaemon-launch-helper	À désactiver quand D-BUS n'est pas utilisé.
/usr/lib/openssh/sshkeysign	À désactiver.
/usr/lib/pt_chown	À désactiver (permet de changer le propriétaire des PTY avant l'existence de devfs).
/usr/libexec/utempter/utempter	À désactiver si le profil utempter SELinux n'est pas utilisé.
/usr/sbin/exim4	À désactiver si Exim n'est pas utilisé.
/usr/sbin/suexec	À désactiver si le suexec Apache n'est pas utilisé.
/usr/sbin/traceroute	(IPv4) Idem ping.
/usr/sbin/traceroute6	(IPv6) Idem ping

Pour rappel voici les commandes pour désactiver les setuid et les setgid :

- Pour désactiver setuid : `chmod u-s <<mon_fichier>>`
- Pour désactiver setgid : `chmod g-s <<mon_fichier>>`

Analyse : Voici une commande maison pour refaire le listing précédent en filtrant sur les fichiers qui sont dans les recommandations :

```
find / -type f -perm /6000 -ls 2>/dev/null | grep -E
'/bin/mount|/bin/netreport|/bin/ping6|/bin/ping|/bin/su|/bin/umount|/sbin/mount.nfs4|/sb
in/mount.nfs|/sbin/umount.nfs4|/sbin/umount.nfs|/sbin/unix_chkpwd|/usr/bin/at|/usr/bin/c
hage|/usr/bin/chfn|/usr/bin/chsh|/usr/bin/crontab'
```

Résultat :

```
root@debian:~# find / -type f -perm /6000 -ls 2>/dev/null | grep -E
'/bin/mount|/bin/netreport|/bin/ping6|/bin/ping|/bin/su|/bin/umount|/sbin/mount.nfs4|/sb
in/mount.nfs|/sbin/umount.nfs4|/sbin/umount.nfs|/sbin/unix_chkpwd|/usr/bin/at|/usr/bin/c
hage|/usr/bin/chfn|/usr/bin/chsh|/usr/bin/crontab'
   650330     52 -rwsr-xr-x   1 root     root          52880 févr.  7  2020
/usr/bin/chsh
   653959     72 -rwsr-xr-x   1 root     root          71912 juil. 28 21:09 /usr/bin/su
   650329     60 -rwsr-xr-x   1 root     root          58416 févr.  7  2020
/usr/bin/chfn
   654248     56 -rwsr-xr-x   1 root     root          55528 juil. 28 21:09
/usr/bin/mount
   654250     36 -rwsr-xr-x   1 root     root          35040 juil. 28 21:09
/usr/bin/umount
   650328     80 -rwxr-sr-x   1 root     shadow        80256 févr.  7  2020
/usr/bin/chage
   663335    180 -rwsr-x---   1 root     sudogrp      182600 févr. 27  2021
/usr/bin/sudo
   655677     44 -rwxr-sr-x   1 root     crontab       43568 févr. 22  2021
/usr/bin/crontab
   650313     40 -rwxr-sr-x   1 root     shadow        38912 juil.  9 18:55
/usr/sbin/unix_chkpwd
```

Partitionnement fin avec droits restreints

R12 (-IRE) : Partitionnement type

Nous avons vu précédemment qu'il est intéressant d'avoir les logs sur une partition dédiée pour éviter (par exemple par une erreur de configuration) que par une augmentation soudaine de ces derniers ils utilisent toute la place disponible sur la partition, qu'il ne soit plus possible de créer des fichiers et que tout cela empeche le bon fonctionnement du système.

Sur la même logique, on peut définir une stratégie de partitionnement ajustable suivant les besoins de nos utilisateurs.
Le partitionnement type recommandé est le suivant :

Point de montage	**Options**	**Description**
/		Partition racine, contient le reste de l'arborescence.
/boot	nosuid,nodev,noexec (noauto optionnel)	Contient le noyau et le chargeur de démarrage. Pas d'accès nécessaire une fois le boot terminé (sauf mise à jour).
/opt	nosuid,nodev (ro optionnel)	Packages additionnels au système. Montage en lecture seule si non utilisé.
/tmp	nosuid,nodev,noexec	Fichiers temporaires. Ne doit contenir que des éléments non exécutables. Nettoyé après redémarrage ou préférablement de type tmpfs.
/srv	nosuid,nodev (noexec,ro optionnels)	Contient des fichiers servis par un service type web, ftp, etc.
/home	nosuid,nodev,noexec	Contient les HOME utilisateurs. Montage en lecture seule si non utilisé.
/proc	hidepid=2	Contient des informations sur les processus et le système.
/usr	nodev	Contient la majorité des utilitaires et fichiers système.

Point de montage	Options	Description
/var	nosuid,nodev,noexec	Partition contenant des fichiers variables pendant la vie du système (mails, fichiers PID, bases de données d'un service).
/var/log	nosuid,nodev,noexec	Contient les logs du système.
/var/tmp	nosuid,nodev,noexec	Fichiers temporaires conservés après extinction.

La commande `mount` sans argument permet de lister l'ensemble des partitions et leurs options de montage.

R13 (--RE) : Restrictions d'accès sur le dossier /boot

Cas particulier : `/boot` , il est fortement recommandé que cette partition soit uniquement accessible (et possédée) par root.
Rappel : pour voir les droits, on peut utiliser la commande `ls -ld /boot` :

```
root@debian:~# ls -ld -d /boot
drwxr-xr-x 4 root root 1024 sept. 29 09:34 /boot
```

Analyse : dans notre situation tout est bon car c'est l'utilisateur root et le groupe root qui possèdent le dossier.

Exemples :

- Serveur web : Pour ce type de serveur, il faut principalement alouer de l'espace mémoire au point de montage `/srv` pour la partie web et `/var` pour tout ce qui va être logs, mails, base de donnée de l'application web.
- Serveur de log : Pour ce type de serveur, il faut principalement alouer de l'espace mémoir au point de montage`/var/log` pour permettre une journalisation impotantes des logs.

Configuration sécurisée services

R21 (-IRE) : Durcissement et surveillance des services soumis à des flux arbitraires

Certains services possédant un système d'authentification peuvent posséder des failles et/ou des vulnérabilités avant cette étape. Par exemple, un serveur utilisant une authentification HTTP basique peut être attaqué de différentes manières. Il faut donc surveiller ces services vulnérables et avertir en cas d'écart au fonctionnement normal de ce dernier.

Pour cela nous utiliserons **Nagios**, un logiciel réalisant de la surveillance système et réseau. Pour installer ce logiciel vous devrez exécutez les commandes suivantes :

```
# Installation des paquets indispensables au bon fonctionnement de Nagios
apt install -y build-essential apache2 php openssl perl make php-gd libapache2-mod-php
libperl-dev libssl-dev daemon wget apache2-utils unzip

# Création d'un compte et d'un groupe pour Nagios
useradd nagios
groupadd nagcmd
usermod -a -G nagcmd nagios
usermod -a -G nagcmd www-data
```

```
# Téléchargement de Nagios
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
tar -zxvf nagios-4.4.6.tar.gz

# Installation et compilation de Nagios
cd /tmp/nagios-4.4.6/
./configure --with-nagios-group=nagios --with-command-group=nagcmd --with-
httpd_conf=/etc/apache2/sites-enabled/
make all
make install
make install-init
make install-config
make install-commandmode
make install-webconf
```

Cependant, pour utiliser **Nagios** nous devons utiliser un hôte distant. Cet hôte devra être configuré afin de pouvoir surveiller les ports associés aux services que l'on souhaite surveiller. Tout d'abord nous devons le définir de la manière suivante :

```
define host{
    use     generic-host            ; Valeur par défaut
    host_name       remotehost      ; Nom de la machine
    alias       Some Remote Host    ; Alias de cette machine
    address     192.168.1.50        ; Adresse IP de la machine a surveillé
    hostgroups      allhosts        ; Groupe auquel elle est associée
}
```

Cette définition peut être placé dans n'importe quel fichier de configuration objet (*.cfg*) sur l'hôte distant.

Après avoir configuré notre hôte, nous devons lui indiqué quels services il doit surveiller et ce qu'il doit surveiller sur chacun de ces services. Nous devons alors définir des services de la manière suivante :

```
define service{
    use     generic-service     ; Valeur par défaut
    host_name       remotehost  ; Noms de la machine
    service_description Product Download Link   ; Description du service surveillé
    check_command   check_http!-u /download/index.php -t 5 -s "latest-version.tar.gz"
; Commande permettant la surveillance
}
```

Cette définition permet de surveiller le service HTPP. La définition ci-dessus permet simplement de vérifier que le fichier l'URI de `/download/index.php` contient la chaîne de charactères `latest-version.tar.gz`. Un autre exemple de définition de service est présenté ci-dessous.

```
define service{
    use     generic-service
    host_name       remotehost
    service_description Special FTP
    check_command   check_ftp!-p 1023 -t 5 -e "Pure-FTPd [TLS]"
}
```

Cette fois-ci nous surveillons le service FTP et plus spécifiquement sur le port 1023. Une alerte est envoyé si le serveur ne répond pas dans les 5 secondes ou si la réponse du serveur ne contient pas la chaîne de charactères `Pure-FTPd [TLS]`.

Une grande partie des services les plus connus possèdent un plugin permettant de les surveiller. Afin d'installer ces plugins nous devons définir les commandes qu'ils utilisent dans un fichier `.cfg` de la manière suivante :

```
define command{
    name        check_http
    command_name    check_http
    command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
}
```

La liste des plugins disponibles et les commandes associées est disponible sur la documentation de **Nagios**.

Une fois la configuration terminé il ne nous reste plus qu'à démarrer ou redémarrer **Nagios** à l'aide des commandes suivantes

```
# Démarrer Nagios pour la 1ère fois
/etc/rc.d/init.d/nagios start

# Redémarrer Nagios après un changement de configuration
/etc/rc.d/init.d/nagios reload
```

R22 (-IRE) : Paramétrage des sysctl système

Sysctl est une interface permettant d'examiner et de modifier dynamiquement les paramètres d'un système d'exploitation Linux. Elle se présente sous la forme de règles que l'on peut ajouter selon nos besoins. Ces règles peuvent permettre de modifier les paramètres systèmes, mais également les paramètres réseaux du système d'exploitation. La liste des règles disponibles peut être afficher à l'aide de la commande `sysctl -a`.

Les règles décrites ci-dessous sont recommandées par l'ANSSI pour un hôte serveur n'ayant pas à effectuer de routage et ayant une configuration IPv6 minimaliste. Ces règles doivent être ajoutées au fichier `/etc/sysctl.conf`, à la suite des règles déjà présentes :

```
# Pas de routage entre les interfaces
net.ipv4.ip_forward = 0

# Filtrage par chemin inverse
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ne pas envoyer de redirections ICMP
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Refuser les paquets de source routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Ne pas accepter les ICMP de type redirect
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

# Loguer les paquets ayant des IPs anormales
net.ipv4.conf.all.log_martians = 1

# RFC 1337
net.ipv4.tcp_rfc1337 = 1

# Ignorer les réponses non conformes à la RFC 1122
```

```
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Augmenter la plage pour les ports éphémères
net.ipv4.ip_local_port_range = 32768 65535

# Utiliser les SYN cookies
net.ipv4.tcp_syncookies = 1

# Désactiver le support des "router solicitations"
net.ipv6.conf.all.router_solicitations = 0
net.ipv6.conf.default.router_solicitations = 0

# Ne pas accepter les "router preferences" par "router advertisements"
net.ipv6.conf.all.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0

# Pas de configuration auto des prefix par "router advertisements"
net.ipv6.conf.all.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_pinfo = 0

# Pas d'apprentissage du routeur par défaut par "router advertisements"
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_defrtr = 0

# Pas de configuration auto des adresses à partir des "router advertisements"
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.default.autoconf = 0

# Ne pas accepter les ICMP de type redirect
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Refuser les packets de source routing
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

# Nombre maximal d'adresses autoconfigurées par interface
net.ipv6.conf.all.max_addresses = 1
net.ipv6.conf.default.max_addresses = 1
```

Si **IPv6** n'est pas utilisé sur le serveur il convient d'ajouter la ligne suivante dans le fichier :

```
# Désactivation d'IPv6
net.ipv6.conf.all.disable_ipv6
```

R23 (-IRE) : Paramétrage des sysctl système

Les règles présentées ci-dessous sont les règles recommandées par l'ANSSI pour tout type de machine. Ces règles doivent également être ajoutées au fichier `/etc/sysctl.conf`, à la suite des règles décrites précédemment :

```
# Désactivation des SysReq
kernel.sysrq = 0

# Pas de core dump des exécutables setuid
fs.suid_dumpable = 0
```

```
# Interdiction de déréférencer des liens vers des fichiers dont
# l'utilisateur courant n'est pas le propriétaire
# Peut empêcher certains programmes de fonctionner correctement
fs.protected_symlinks = 1
fs.protected_hardlinks = 1

# Activation de l'ASLR
kernel.randomize_va_space = 2

# Interdiction de mapper de la mémoire dans les adresses basses (0)
vm.mmap_min_addr = 65536

# Espace de choix plus grand pour les valeurs de PID
kernel.pid_max = 65536

# Obfuscation des adresses mémoire kernel
kernel.kptr_restrict = 1

# Restriction d'accès au buffer dmesg
kernel.dmesg_restrict = 1

# Restreint l'utilisation du sous système perf
kernel.perf_event_paranoid = 2
kernel.perf_event_max_sample_rate = 1
```

Il est également possible d'ajouter une règle permettant d'interdire le chargement de nouveaux modules, y compris par l'utilisateur *root*. Cependant, même si cette mesure est très efficace en terme de sécurité elle peut également avoir de lourdes conséquences sur le fonctionnement du système. Il est recommandé d'intégrer cette règle aux scripts de démarrage du système afin qu'elle soit appliquée le plus rapidement possible.

Règles iptables pour trafic entrant

Pour contrer les attaques sur notre machine, on va installer un parefeu. Nous allons utiliser `iptables` pour filtrer ce qu'il est possible de faire depuis le réseau sur notre machine.

Installer iptables : `apt install iptables`
Exécuter iptables : `sudo iptables` (ne pas oublier `sudo`)

Explication brève des règles iptables :

- INPUT : paquet en direction de la machine => filtre INPUT.
- OUTPUT : paquet en provenance de la machine => filtre OUTPUT.
- ACCEPT => autorisé à passer.
- REJECT => renvoie un paquet erroné en réponse au paquet qui correspond (envoie un message donc non furtif).
- DROP => paquet détruit (furtif)

Règles dans /etc/init.d/iptables.custom.rules :

```
# Règles par défaut
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [687:218631]

# Autorise le traficinterne sur une loopback
-A INPUT -i lo -j ACCEPT
```

```
# Drop les paquets non conformes, comme les headers mals formés, etc.
-A INPUT -m state --state INVALID -j DROP

# Autorise les paquets ESTABLISHED et RELATED
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Autorise tout pour les IP spécifiées (admin)
-A INPUT -s 192.168.122.1 -j ACCEPT
-A INPUT -s 10.2.152.92 -j ACCEPT

# Autorise le traffic sur les ports spécifiés
# 22 ssh
# 25 smtp : sortie email
# 110 pop3 : entrée email
# 143 imap : entrée email
-A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 110 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 143 -j ACCEPT

# Autorise les paquets ICMP utiles
# Note: La RFC 792 statue que tous les hosts doivent répondre aux requêtes ICMP ECHO.
# Bloquer ces paquets peut rendre les diagnostics simple plus compliqués.
# La vraie sécurité réside dans le verrouillage et le renforcement de tous les services,
et non en se cachant.
-A INPUT -p icmp --icmp-type 0  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 3  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 8  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 11 -m conntrack --ctstate NEW -j ACCEPT

# Drop tous les les paquets entrants NULL mals formés
-A INPUT -p tcp --tcp-flags ALL NONE -j DROP

# Drop les paquets d'attaque syn-flood
-A INPUT -p tcp ! --syn -m state --state NEW -j DROP

# Drop les paquets entrants XMAS mals formés
-A INPUT -p tcp --tcp-flags ALL ALL -j DROP

# Rejete le trafique autre que les règles mentionnées au dessus
-A INPUT -j DROP

# Valider les modifications
COMMIT
```

Par défaut, il faut recharger les règles iptables après chaque redémarrage, pour remedier à ce problème et à de potentielles erreurs (oubli au démarrage du serveur de charger la configuration par exemple), il est possible d'automatiser cela :

Éditer le fichier `/etc/network/interfaces` et ajouter la ligne :

```
post-up iptables-restore < /etc/init.d/iptables.custom.rules
```

Après la ligne :

```
iface lo inet loopback
```

À chaque fois que l'interface réseau de loopback sera allumée, les règles seront ajoutées.

Voilà le récapitulatif des règles (`sudo iptables -L`) :

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             state INVALID
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  dell-2               anywhere
ACCEPT     all  --  10.2.152.92          anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:smtp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:pop3
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:imap2
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp destination-
unreachable ctstate NEW
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded ctstate
NEW
DROP       tcp  --  anywhere             anywhere             tcp
flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere             anywhere             tcp
flags:!FIN,SYN,RST,ACK/SYN state NEW
DROP       tcp  --  anywhere             anywhere             tcp
flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PSH,ACK,URG
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Note : Pour supprimer toutes les règles iptables si une erreur a été faite, il faut faire les commandes suivantes :

```
sudo iptables -F
sudo iptables -X
sudo iptables -t nat -F
sudo iptables -t nat -X
sudo iptables -t mangle -F
sudo iptables -t mangle -X
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT
```

Note : Pour lister l'ensemble des règles, on exécute la commande :

```
sudo iptables -L
```

Note : Pour bannir une adresse IP, il faut faire la commande suivante :

```
sudo iptables -I INPUT 1 -s 1.2.3.4 -j DROP
```

Note : Pour un serveur web, il faut généralement autoriser les ports 80 (http) et 443 (https) car ils écoutent sur ces ports pour délivrer du contenu. Il ne faut surtout pas oublier d'ouvrir tous les ports nécessaires au bon fonctionnement des services proposés par un serveur sous peine d'avoir les fonctionnalités proposées hors-ligne.

Niveau de sécurité : RENFORCÉ

Écriture de scripts d'audit spécialisés

R35 (--RE) : Valeur de umask

Sous Linux, les droits d'accès sont gérés par "controle d'accès discrétionnaire". C'est à dire que c'est au propriétaire du fichier de définir les droits d'accès.

Quand un utilisateur n'est pas explicite dans sa demande de droits, Linux y applique un masque (umask). Par défaut, ce masque est très permissif (`0022`) ce qui implique que tout fichier créé est lisible par tous les utilisateurs.
L'ANSSI recommande de définir le umask système à `0027`. Ce qui signifie que tout fichier créé est lisible uniquement par le propriétaire et son groupe, ainsi que modifiable uniquement par le propriétaire.
La recommandation de l'ANSSI pour le umask utilisateur est `0077` : tout fichier créé par un utilisateur n'est lisible et modifiable que par lui.

Pour changer le umask pour les utilisateurs, il faut éditer le fichier `/etc/profile` et y ajouter la ligne suivante :

```
umask 0077
```

Vérification :
J'ai créé un fichier "test" vide avant le changement du fichier `/etc/profile` et un fichier "test2" après, voici le résultat sur les droits :

```
-rw-r--r-- 1 clement clement    0 oct.  13 08:55 test
-rw------- 1 clement clement    0 oct.  13 08:55 test2
```

Cela prouve que la directive a bien été mise en place.

Pour le umask système, cela dépend de la distribution. Dans Debian il peut se trouver dans `/etc/init.d/rc`, dans CentOS `/etc/sysconfig/init` et sinon dans un fichier de configuration de `systemd`.

Il faut faire attention aux droits des fichiers qui rentrent dans les catégories suivantes :

- Fichier contenant des éléments secrets (mots de passes, informations confidentielles, ...)
- Fichier exécutable avec des droits particuliers comme setuid ou setgid
- Dossier auxquel tout le monde a accès
- Fichier IPC nommé (comme les sockets ou pipes)

R36(-IRE) : Droits d'accès aux fichiers de contenu sensible

Les fichiers à contenu sensibles doivent posséder des droits encore plus restreints. Il est recommandé qu'ils ne soient lisibles que par root.
Les fichiers dits "publiques" sont eux lisibles par tous mais modifiables uniquement par root.

Exemple :

```
root@debian:/etc/init.d# ls -lah /etc/*shadow
-rw-r----- 1 root shadow 698 sept. 29 09:20 /etc/gshadow
-rw-r----- 1 root shadow 966 sept. 20 09:19 /etc/shadow
root@debian:/etc/init.d# ls -lah /home/clement/.ssh/id_rsa
-rw------- 1 clement clement 4 oct.  13 09:06 /home/clement/.ssh/id_rsa
```

Voici le schéma d'analyse proposé par l'ANSSI :

1. Les fichiers systèmes sensibles doivent avoir comme propriétaire le compte root afin d'éviter qu'un changement de droits puisse être effectué par un utilisateur non privilégié ;
2. Quand ce fichier doit être accessible à un utilisateur non root (exemple : base de mot de passe de serveur web), l'utilisateur associé au serveur doit être membre d'un groupe dédié (exemple : www-group) qui aura un droit d'accès en lecture seule à ce fichier ;
3. Le reste des utilisateurs ne doit posséder aucun droit.

Optionnel : Fichiers sans utilisateur ou groupe propriétaire

Les fichiers sans utilisateur ou groupe propriétaire doivent être :

- assignés à un utilisateur/groupe qui existe si on souhaite conserver le fichier
- supprimés

Pour trouver les fichiers qui répondent aux deux conditions (pas d'utilisateur et pas de groupe propriétaire) on peut utiliser la commande : `find / -type f \( -nouser -o -nogroup \) -ls 2>/dev/null`

R39 (-IRE) : Répertoires temporaires dédiés aux comptes

Tous les utilisateurs ont accès à un zone de stockage temporaire (dont le contenu est supprimé à la fermeture de session par exemple). Ces zones permettent d'enregistrer des données pour les partager entre processus par exemple.
Le danger est que tout le monde ayant accès à ces zones, les fichiers temporaires d'un utilisateur A peuvent être exploités par un utilisateur B pour abuser des droits de A, usurper son identité ou faire une attaque par "élévation de privilèges".

Une bonne pratique est d'avoir une zone de stockage temporaire PAR UTILISATEUR.

Pour faire cela, on peut mettre en place le module pam_namespace.

Premièrement, vérifier qu'il existe un fichier `/etc/security/namespace.init` non vide.
Ensuite décommenter les trois dernières lignes du fichier `/etc/security/namespace.conf` afin d'avoir un fichier similaire à ça :

```
/tmp     /tmp-inst/               level      root,adm
/var/tmp /var/tmp/tmp-inst/     level      root,adm
$HOME    $HOME/$USER.inst/          level
```

Il faut ensuite charger le module dans PAM :
Éditer le fichier `/etc/pam.d/login` et ajouter la ligne :

```
session    required     pam_namespace.so
```

Il reste à redémarrer la machine et normalement /tmp devrait avoir une nouvelle structure de dossiers :

```
root@debian:~# tree /tmp
/tmp
└── user
    ├── 0
    └── 1000
```

La nouvelle structure est /tmp/user/<<id_user>>.

R40 (-IRE) : Sticky bit et droits d'accès en écriture

Les dossiers accessibles en écriture par tous les utilisateurs doivent avoir avoir le sticky bit activé.

Pour lister les répertoires pour lesquels tous les utilisateurs ont les droits d'écriture mais pour lesquels le sticky bit n'est pas activé on peut utiliser la commande suivante : `find / -type f -perm -0002 -ls 2>/dev/null`.
Si tout est bon, la commande ne renvoie rien.

Par ailleurs, il est recommandé que les dossiers accessibles en écriture par tous les utilisateurs doivent être possédés par root.

Pour lister les répertoires pour lesquels tous les utilisateurs ont les droits d'écriture mais pour lesquels le propriétaire n'est pas root on peut utiliser la commande suivante : `find / -type d -perm -0002 -a \ ! -uid 0 -ls 2>/dev/null`.
À nouveau, la commande ne renvoie rien si tout est ok.

Important : Aucun fichier non temporaire n'a vocation à être modifiable par tous. Quand un fichier doit être modifiable par plusieurs utilisateurs, il faut créer un groupe et ajouter les utilisateur à ce groupe, puis donner les droits de modification au groupe.

Pour lister les fichiers modifiables par tous on peut utiliser la commande : `find / -type f -perm -0002 -ls 2>/dev/null`
Dans notre situation, les fichiers sont regroupables en trois catégories :

- /proc/sys/...
- /proc/<>/...
- /sys/kernel/...

Analyse : ces trois types de fichiers sont temporaires et seront supprimés au redémarrage, il n'y a donc pas de problème dans notre situation.

R41 (-IRE) : Sécurisation des accès pour les sockets et pipes nommées

Les applications d'un système peuvent échanger des données via des sockets. Ces sockets fonctionnent au niveau IP du modèle OSI.
Sur Linux il existe aussi les pipes et et les sockets locaux.
Les sockets et pipes n'ont pas de droits d'accès, leurs droits d'accès sont ceux du dossier les contenant. Il faut donc faire attention à ces droits.

Pour lister l'ensemble des sockets locaux, on peut utiliser la commande : `ss`.
Pour lister l'ensemble des sockets locaux et les processus associés, on peut utiliser la commande : `ss -xp`.

Pour lister les mémoires partagées et leurs droits d'accès, on peut utiliser la commande : `ipcs` pour la mémoire et `ls /dev/shm` pour les droits.

Pour lister les informations détaillé sur les I/O et IPC du système, on peut utiliser la commande : `lsof`.

Une règle importante est que les sockets locaux ne soient pas créés à la racine d'un répertoire temporaire accessible en écriture à tous.

Suppression des programmes innutiles

R1 (MIRE) : Minimisation des services installés

Afin de minimiser la surface attaquable de notre système et ne pas maintenir des paquets innutilement et perdre du temps, il est important de superviser les services et paquets installés. Il faut se limiter au stricte nécessaire : il faut pouvoir justifier la présence de ceux-ci ou alors ils doivent être supprimés.

Quelques commandes utiles :

Commande	**Description**
`systemctl stop <<service_name>>`	Arret d'un service
`systemctl disable <<service_name>>`	Désactiver un service
`apt remove <<package_name>>`	Retirer un package
`apt purge <<package_name>>`	"Purger" un package : retire le package, ses fichiers et ses dépendances
`apt autoremove <<package_name>>`	Retirer les dépendances non utilisées
`systemctl daemon-reload`	Redémarrer le daemon systemd

R2 (MIRE) : Minimisation de la configuration

De la même manière que la règle précedente, pour éviter d'augmenter la charge de travail de l'administrateur dans la maintenance, le debug et dans le développement du système, il faut éviter d'avoir des configurations trop compliquées/lourdes si on peut s'en passer.

Nous ajouterons qu'il faut penser à documenter les processus de configuration des services, commenter les configurations afin de se souvenir des paramètres changés et garder des fichiers de configuration "propres" (bien rédigés, bien documentés, simples, bien indentés, ...).

Pour lister les services en cours d'exécution on peut faire : `systemctl list-units --type=service --state=running`

La commande retourne un résultat comme celui-ci :

```
root@debian:/etc/init.d# systemctl --type=service --state=running
  UNIT                     LOAD   ACTIVE SUB     DESCRIPTION
```

```
  cron.service              loaded active running Regular background program processing
daemon
  dbus.service              loaded active running D-Bus System Message Bus
  getty@tty1.service        loaded active running Getty on tty1
  rsyslog.service           loaded active running System Logging Service
  ssh.service               loaded active running OpenBSD Secure Shell server
  systemd-journald.service  loaded active running Journal Service
  systemd-logind.service    loaded active running User Login Management
  systemd-timesyncd.service loaded active running Network Time Synchronization
  systemd-udevd.service     loaded active running Rule-based Manager for Device Events
and Files
  user@1000.service         loaded active running User Manager for UID 1000
  wpa_supplicant.service    loaded active running WPA supplicant

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.
11 loaded units listed.
```

Analyse : La présence de tous nos services en cours d'exécution est justifiable donc notre système respecte ces deux dernières règles.

Par ailleurs, il faut faire attention dans nos fichiers de configuration à ne pas activer des fonctionnalités qui ne sont pas nécessaires à l'utilisateur/au bon fonctionnement du système. Une fois de plus, cela reviendrait à augmenter la surface attaquable de notre système innutilement.

Blocage du chargement dynamique de modules

R24 (--RE) : Désactivation du chargement des modules noyau

Sysctl est une interface permettant d'examiner et de modifier dynamiquement les paramètres d'un système d'exploitation Linux. Elle se présente sous la forme de règles que l'on peut ajouter selon nos besoins. Ces règles peuvent permettre de modifier les paramètres systèmes, mais également les paramètres réseaux du système d'exploitation. La liste des règles disponibles peut être afficher à l'aide de la commande `sysctl -a`.

Il est possible d'ajouter une règle permettant d'interdire le chargement de nouveaux modules, y compris par l'utilisateur *root*. Cependant, même si cette mesure est très efficace en terme de sécurité elle peut également avoir de lourdes conséquences sur le fonctionnement du système. Cette doit être ajouté au fichier `/etc/sysctl.conf`.

```
# Interdiction de chargement de nouveaux modules
kernel.modules_disabled = 1
```

R25 (--RE) : Configuration sysctl du module Yama

L'appel système **ptrace** permet de tracer le fonctionnement de processus. Par défaut, un utilisateur pourra tracer le fonctionnement de tous les processus lui appartenant, notamment des processus pouvant stocker des données sensibles (les navigateurs internet, ssh-agent, ...).

Yama est un module de sécurité permettant de contrôler les droits d'accès à cet appel système. La règle devra être configuré de la manière suivante, en fonction des besoins, dans le fichier `/etc/sysctl.conf` :

```
# Restriction sur l'utilisation de ptrace.
# Les utilistaneurs pourront tracer leurs processus parents
kernel.yama.ptrace_scope = 1

# Seuls les administrateurs pourront utiliser ptrace
kernel.yama.ptrace_scope = 2

# Aucun processus ne pourra être tracer en utilisant ptrace.
# Un redémarrage est nécessaire pour modifier cette règle à nouveau.
kernel.yama.ptrace_scope = 3
```

Il est également recommandé de charger **Yama** au démarrage de la machine. Pour ce faire, il faut ajouter la ligne suivante au fichier `/boot/grub/grub.cfg` :

```
security=yama
```

Pour vérifier si la règle est bien mise en place il suffit d'utiliser la commande :

```
cat /proc/sys/kernel/yama/ptrace_scope
```

Configuration sécurisée système

R22 (-IRE) : Paramétrage des sysctl système

Les règles décrites ci-dessous sont recommandées par l'ANSSI pour un hôte serveur n'ayant pas à effectuer de routage et ayant une configuration IPv6 minimaliste. Ces règles doivent être ajoutées au fichier `/etc/sysctl.conf`, à la suite des règles déjà présentes :

```
# Pas de routage entre les interfaces
net.ipv4.ip_forward = 0

# Filtrage par chemin inverse
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ne pas envoyer de redirections ICMP
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Refuser les paquets de source routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Ne pas accepter les ICMP de type redirect
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

# Loguer les paquets ayant des IPs anormales
net.ipv4.conf.all.log_martians = 1

# RFC 1337
net.ipv4.tcp_rfc1337 = 1
```

```
# Ignorer les réponses non conformes à la RFC 1122
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Augmenter la plage pour les ports éphémères
net.ipv4.ip_local_port_range = 32768 65535

# Utiliser les SYN cookies
net.ipv4.tcp_syncookies = 1

# Désactiver le support des "router solicitations"
net.ipv6.conf.all.router_solicitations = 0
net.ipv6.conf.default.router_solicitations = 0

# Ne pas accepter les "router preferences" par "router advertisements"
net.ipv6.conf.all.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0

# Pas de configuration auto des prefix par "router advertisements"
net.ipv6.conf.all.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_pinfo = 0

# Pas d'apprentissage du routeur par défaut par "router advertisements"
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_defrtr = 0

# Pas de configuration auto des adresses à partir des "router advertisements"
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.default.autoconf = 0

# Ne pas accepter les ICMP de type redirect
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Refuser les packets de source routing
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

# Nombre maximal d'adresses autoconfigurées par interface
net.ipv6.conf.all.max_addresses = 1
net.ipv6.conf.default.max_addresses = 1
```

Si **IPv6** n'est pas utilisé sur le serveur il convient d'ajouter la ligne suivante dans le fichier :

```
# Désactivation d'IPv6
net.ipv6.conf.all.disable_ipv6
```

R23 (-IRE) : Paramétrage des sysctl système

Les règles présentées ci-dessous sont les règles recommandées par l'ANSSI pour tout type de machine. Ces règles doivent également être ajouté au fichier `/etc/sysctl.conf`, à la suite des règles décrites précédemment :

```
# Désactivation des SysReq
kernel.sysrq = 0

# Pas de core dump des exécutables setuid
```

```
fs.suid_dumpable = 0

# Interdiction de déréférencer des liens vers des fichiers dont
# l'utilisateur courant n'est pas le propriétaire
# Peut empêcher certains programmes de fonctionner correctement
fs.protected_symlinks = 1
fs.protected_hardlinks = 1

# Activation de l'ASLR
kernel.randomize_va_space = 2

# Interdiction de mapper de la mémoire dans les adresses basses (0)
vm.mmap_min_addr = 65536

# Espace de choix plus grand pour les valeurs de PID
kernel.pid_max = 65536

# Obfuscation des adresses mémoire kernel
kernel.kptr_restrict = 1

# Restriction d'accès au buffer dmesg
kernel.dmesg_restrict = 1

# Restreint l'utilisation du sous système perf
kernel.perf_event_paranoid = 2
kernel.perf_event_max_sample_rate = 1
```

Journalisation de l'activité par auditd

R50 (--RE) : Journalisation de l'activité par auditd

Auditd est un service de journalisation permettant d'enregistrer des opérations système et d'alerter un administrateur lorsque des opérations non prévues ont lieu. Ce service permet de surveiller de nombreuses actions, notamment les appels système, les accès à des fichiers ou l'ajout de modules.

Dans un premier temps nous devrons installer le package *auditd* à l'aide de la commande suivante :

```
apt install -y auditd
```

Afin de pouvoir commencer à auditer les processus le plus rapidement possible nous devons ajouter un argument lors du démarrage du système. Pour ce faire, il faut ajouter la ligne suivante au fichier `/boot/grub/grub.cfg` :

```
audit=1
```

Une fois cela fait, nous pouvons commencer à configurer **auditd** afin de surveiller les actions souhaitées. Les règles suivantes sont celles proposées par l'ANSSI et permettent un audit des fonctionnalités à surveiller. Ces règles doivent être ajoutées au fichier `/etc/audit/rules.d/audit.rules` (le paramètre *-k* permet d'afficher les recherches dans le fichier de logs) :

```
# Exécution de insmod,rmmod et modprobe
-w /sbin/insmod -p x -k audit_modules
-w /sbin/modprobe -p x -k audit_modules
-w /sbin/rmmod -p x -k audit_modules
```

```
# Journaliser les modifications dans /etc/ et /root/
-w /etc/ -p wa -k audit_conf
-w /root/ -p rwxa -k audit_root

# Surveillance de montage/démontage
-a exit,always -S mount -S umount2 -k audit_mount

# Appels de syscalls x86 suspects
-a exit,always -S ioperm -S modify_ldt -k audit_syscall

# Appels de syscalls qui doivent être rares et surveillés de près
-a exit,always -S get_kernel_syms -S ptrace -S prctl -k audit_syscall

# Rajout du monitoring pour la création ou suppression de fichiers
-a exit,always -F arch=b64 -S unlink -S rmdir -S rename –k audit_files
-a exit,always -F arch=b64 -S creat -S open -S openat -F exit=-EACCESS –k audit_files
-a exit,always -F arch=b64 -S truncate -S ftruncate -F exit=-EACCESS –k audit_files
```

Une fois les règles ajoutées il nous reste plus qu'à redémarrer **auditd**. Les logs générés par ce service se trouvent dans le fichier `/var/log/audit/audit.log`.

Règles iptables pour trafic local et sortant

⚠️ Il est nécessaire d'avoir lu et mis en place la partie "Règles iptables pour trafic entrant" avant de lire celle ci.

Maintenant que nous avons sécurisé en trafic entrant sur notre système, nous pouvons aussi sécuriser le trafic local et sortant.

Pour le trafic sortant, le plus simple est de limiter aux mêmes règles que pour le trafic entrant, puisque nos besoins sont les mêmes.
Il y a quelques ports que l'on peut autoriser en plus : telnet (port 23), dns (port 53 TCP|UDP), http (port 80), https (port 443)

Voici le nouveau fichier `/etc/init.d/iptables.custom.rules` :

```
# Règles par défaut
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:OUTPUT ACCEPT [687:218631]

# Autorise le traficinterne sur une loopback
-A INPUT -i lo -j ACCEPT

# Drop les paquets non conformes, comme les headers mals formés, etc.
-A INPUT -m state --state INVALID -j DROP

# Autorise les paquets ESTABLISHED et RELATED
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Autorise tout pour les IP spécifiées (admin)
-A INPUT -s 192.168.122.1 -j ACCEPT
-A INPUT -s 10.2.152.92 -j ACCEPT

# Autorise le traffic sur les ports spécifiés
# 22 ssh
# 25 smtp : sortie email
```

```
# 110 pop3 : entrée email
# 143 imap : entrée email
-A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 110 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 143 -j ACCEPT

# 53 dns/tcp
# 53 dns/udp
# 80 http
# 443 https
-A OUTPUT -p tcp --dport 53 -j ACCEPT
-A OUTPUT -p udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp --dport 443 -j ACCEPT

# Autorise les paquets ICMP utiles
# Note: La RFC 792 statue que tous les hosts doivent répondre aux requêtes ICMP ECHO.
# Bloquer ces paquets peut rendre les diagnostics simple plus compliqués.
# La vraie sécurité réside dans le verrouillage et le renforcement de tous les services,
et non en se cachant.
-A INPUT -p icmp --icmp-type 0  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 3  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 8  -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p icmp --icmp-type 11 -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p icmp --icmp-type 0  -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p icmp --icmp-type 3  -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p icmp --icmp-type 8  -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p icmp --icmp-type 11 -m conntrack --ctstate NEW -j ACCEPT

# Drop tous les les paquets entrants NULL mals formés
-A INPUT -p tcp --tcp-flags ALL NONE -j DROP

# Drop les paquets d'attaque syn-flood
-A INPUT -p tcp ! --syn -m state --state NEW -j DROP

# Drop les paquets entrants XMAS mals formés
-A INPUT -p tcp --tcp-flags ALL ALL -j DROP

# Rejete le trafique autre que les règles mentionnées au dessus
-A INPUT -j DROP

# Valider les modifications
COMMIT
```

Voilà le nouveau récapitulatif des règles (`sudo iptables -L`) :

```
root@debian:/home/clement# sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             state INVALID
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  dell-2               anywhere
ACCEPT     all  --  10.2.152.92          anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:smtp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:pop3
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:imap2
```

```
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp destination-
unreachable ctstate NEW
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded ctstate
NEW
DROP       tcp  --  anywhere             anywhere             tcp
flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere             anywhere             tcp
flags:!FIN,SYN,RST,ACK/SYN state NEW
DROP       tcp  --  anywhere             anywhere             tcp
flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PSH,ACK,URG
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp destination-
unreachable ctstate NEW
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request ctstate
NEW
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded ctstate
NEW
```

Rappel : Pour lister l'ensemble des règles, on exécute la commande :

```
sudo iptables -L
```

Note : Pour interdire la communication (entrant & sortant) avec une adresse IP, il faut faire la commande suivante :

```
sudo iptables -I INPUT 1 -s 1.2.3.4 -j DROP
sudo iptables -I OUTPUT 1 -s 1.2.3.4 -j DROP
```

Note : Pour accepter l'ensemble du trafic local, on peut ajouter ces règles :

```
sudo iptables -I OUTPUT -o eth0 -d 0.0.0.0/0 -j ACCEPT
sudo iptables -I INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Niveau de sécurité : ÉLEVÉ

Confinement par AppArmor

AppArmor est un outil permet d'appliquer une politique du "privilege minimum" : on accorde aux utilisateurs/services/programmes les priveleges minimum requis pour leur travail. AppArmor utilise le principe de MAC : Mandatory Access Control, Contrôle d'accès obligatoire.
Le Contrôle d'accès obligatoire (MAC) est une alternative aux "Contrôle d'accès discrétionnaire" (DAC) et "Contrôle d'accès à base de rôles" (RBAC).
La stratégie de MAC est que les décisions de protection ne doivent pas être prises par le propriétaire des objets concernés.
Le MAC permet d'associer des règles sur les fichiers, processus et utilisateurs.

Installation :

```
apt install apparmor apparmor-utils
```

Une commande utile pour voir l'état du fonctionnement de AppArmor :

```
sudo aa-status
```

Exemple de retour :

```
root@debian:~# sudo aa-status
apparmor module is loaded.
6 profiles are loaded.
6 profiles are in enforce mode.
   /usr/bin/man
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
0 profiles are in complain mode.
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```

R65 (---E) : Activation des profils de sécurité AppArmor

À l'installation sur Debian 11, il existe 6 profils pré-installés :

```
root@debian:~# ls /etc/apparmor.d
abstractions  disable  force-complain  local  lsb_release  nvidia_modprobe  tunables
usr.bin.man
```

Si on veut ajouter des profils par défaut, on peut installer les paquets `apparmor-profiles` et `apparmor-profiles-extra` :

```
apt install apparmor-profiles apparmor-profiles-extra
```

On se retrouve maintenant avec 16 profils installés :

```
abstractions  disable         lsb_release      sbin.syslog-ng  usr.bin.irssi
usr.bin.totem         usr.sbin.avahi-daemon  usr.sbin.mdnsd  usr.sbin.smbd
apache2.d     force-complain  nvidia_modprobe  sbin.syslogd    usr.bin.man
usr.bin.totem-previewers  usr.sbin.dnsmasq   usr.sbin.nmbd   usr.sbin.smbldap-useradd
bin.ping      local       sbin.klogd       tunables        usr.bin.pidgin  usr.sbin.apt-
cacher-ng    usr.sbin.identd    usr.sbin.nscd   usr.sbin.traceroute
```

Pour recevoir lire les logs plus proprement, on peut aussi installer `apparmor-notify`.
Avec `aa-notify` on peut visualiser les notifications et messages de refus de permissions par AppArmor.

Note : AppAmor dispose de trois modes :

- enforcing : restreint l'accès aux fichiers sur la base du profile créé pour l'application
- complain : se charge des logs
- unconfined : aucun logging, pas de restriction

Note : Pour passer un profil de "complain" à "enforce" on utilise la commande : `aa-enforce <<chemin_vers_profil>>`
Pour passer un profil de "enforce" à "complain" on utilise la commande : `aa-complain <<chemin_vers_profil>>`

Note : Regénerer un profil : `aa-cleanprof <<chemin_vers_profil>>`

Optionnel : création d'un nouveau profil

Comme nous venons de le voir, il est possible d'obtenir des profils par défaut fournis par les applications.
Nous allons voir maintenant comment créer un profil personnalisé, pour une application qui n'est fournit pas.

Pour lister les applications non confinées, il faut utiliser la commande : `ps -auxZ | grep '^unconfined'`

Note : Il faut en priorité créer des profils pour les applications qui intéragissent sur le réseau, car elles sont les plus susceptibles d'être attaquées.

Nous allons essayer de créer un profil pour le processus "dhclient" :

```
# aa-genprof dhclient
Writing updated profile for /usr/sbin/dhclient.
Setting /usr/sbin/dhclient to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /usr/sbin/dhclient

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
```

```
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d.

Profile:  /usr/sbin/dhclient
Execute:  /usr/sbin/dhclient-script
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t
/ (F)inish
P
Should AppArmor sanitise the environment when
switching profiles?

Sanitising environment is more secure,
but some applications depend on the presence
of LD_PRELOAD or LD_LIBRARY_PATH.

(Y)es / [(N)o]
Y
Writing updated profile for /usr/sbin/dhclient-script.
Complain-mode changes:

Profile:    /usr/sbin/dhclient
Capability: net_raw
Severity:   8

 [1 - capability net_raw,]
[(A)llow] / (D)eny / (I)gnore / Audi(t) / Abo(r)t / (F)inish
A
Adding capability net_raw to profile.

Profile:  /sbin/dhclient
Capability: net_bind_service
Severity:   8

 [1 - #include <abstractions/nis> ]
  2 - capability net_bind_service,
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
A
Adding #include <abstractions/nis> to profile.

Profile:  /usr/sbin/dhclient
Path:     /etc/ssl/openssl.cnf
New Mode: owner r
Severity: 2

 [1 - #include <abstractions/lightdm>]
  2 - #include <abstractions/openssl>
  3 - #include <abstractions/ssl_keys>
  4 - owner /etc/ssl/openssl.cnf r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) /
(O)wner permissions off / Abo(r)t / (F)inish
2

Profile:  /usr/sbin/dhclient
Path:     /etc/ssl/openssl.cnf
New Mode: owner r
```

```
Severity: 2

  1 - #include <abstractions/lightdm>
 [2 - #include <abstractions/openssl>]
  3 - #include <abstractions/ssl_keys>
  4 - owner /etc/ssl/openssl.cnf r,
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t /
(F)inish / (M)ore
A
[...]
Profile:  /usr/sbin/dhclient-script
Path:     /usr/bin/dash
New Mode: owner r
Severity: unknown

 [1 - #include <abstractions/lightdm>]
  2 - #include <abstractions/ubuntu-browsers.d/plugins-common>
  3 - owner /usr/bin/dash r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) /
(O)wner permissions off / Abo(r)t / (F)inish
A
Adding #include <abstractions/lightdm> to profile.
Deleted 2 previous matching profile entries.

= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/dhclient]
  2 - /usr/sbin/dhclient-script
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean
profiles / Abo(r)t
S
Writing updated profile for /usr/sbin/dhclient.
Writing updated profile for /usr/sbin/dhclient-script.

Profiling: /usr/sbin/dhclient

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
F
Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /usr/sbin/dhclient.
```

On peut vérifier que le profil est bien activé et que le processus est bien confiné avec les commandes données plus tôt.
Le processus est bien confiné.

ALLER PLUS LOIN : BLINDAGE LYNIS

Dans cette partie, nous allons essayer de couvrir le plus de recommandations possibles retournées dans les rapports de Lynis.

Couldn't find 2 responsive nameservers [NETW-2705]

Pourquoi ? Pour limiter l'impact d'un serveur DNS hors ligne, il est important d'avoir un second serveur DNS de renseigné dans notre système pour être certain de toujours pouvoir résoudre les noms de domaines auxquels on veut accéder.

Comment ? Éditer le fichier `/etc/resolv.conf` et ajouter une ligne :

```
nameserver <<adresse_dns>>
```

Par exemple en utilisant l'un des serveurs DNS de Google :

```
nameserver 8.8.8.8
```

This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

Pourquoi ? Pour s'assurer que Lynis est toujours en mesure de détecter les dernières failles et avoir une analyse la plus précise (sans faux-positif, faux-négatif, bugs, ...) il est important de le garder à jour (comme tous logiciels sous notre système d'ailleurs).

Comment ? Installer la dernière version de Lynis (trouvable depuis le dépot officiel).

Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]

Pourquoi ? Le paquet `apt-listbugs` affiche à chaque installation/mise à jour d'un paquet apt s'il contient des failles publiées. Cela permet d'éviter d'installer un paquet qui pourrait mettre en danger notre machine.

Comment ? Installer le paquet apt-listbugs :

```
apt install apt-listbugs
```

Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]

Pourquoi ? Le paquet `needrestart` permet de vérifier que les services utilisent bien les dernières versions des bibliothèques installées. Il se peut qu'une mise à jour ait mis à jour une bibliothèque, mais qu'un service utilise encore l'ancienne version de cette bibliothèque. Le paquet `needrestart` redémarre le service afin qu'il utilise la nouvelle version.

Comment ? Installer le paquet needrestart :

```
apt install needrestart
```

Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]

Pourquoi ? Le paquet `debsums` hash en md5 les fichiers .deb afin de s'assurer de leur intégrité. Cela évite des attaques sur le réseau de type MITM.

Comment ? Installer le paquet debsums :

```
apt install debsums
```

Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

Pourquoi ? Le paquet `fail2ban` bloque automatiquement les machines distantes qui essaient de se connecter et entrent plusieurs fois un mot de passe éronné.

Comment ? Installer le paquet fail2ban :

```
apt install fail2ban
```

Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

Pourquoi ? Le répertoire /boot n'est pas chiffré. Il est d'autant plus important de protéger le GRUB avec un mot de passe pour s'assurer qu'au démarrage de la machine ce sont les bonnes configurations qui sont chargées et qu'un utilisateur non autorisé ne peut pas démarrer la machine.

Comment ? Exécuter la commande `grub-mkpasswd-pbkdf2` pour choisir le mot de passe qui sera demandé au démarrage de grub

```
root@debian:~# grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.970DF860B3F7C4E16F71455C0548E36AC2C2E91406D4DFDE3D07D1F10EDA306
20032595295F54FCE2EDC63A1DDBE57C49B79E4D797A85D0837DC9DA82DE3E9FF.05490494B481DEA8C30F86
397E7ACF698B344AEC2313850B431EA36708BC9A8856532D494FFBD4C8EA0F3DBF64EFAA82389DCBDCD39C60
FD83E2AF7BB539D037
```

Consider hardening system services [BOOT-5264]

Pourquoi ? Pour réduire la surface d'attaque, il est important de renforcer la configuration des services sur notre machine.

Comment ? Vérifier la sécurité des services avec la commande `/usr/bin/systemd-analyze security`.
Voici le résultat sur notre machine :

```
root@debian:~# /usr/bin/systemd-analyze security
UNIT                                  EXPOSURE PREDICATE HAPPY
anacron.service                            9.6 UNSAFE    😨
auditd.service                             8.8 EXPOSED   😕
clamav-freshclam.service                   9.6 UNSAFE    😨
cron.service                               9.6 UNSAFE    😨
dbus.service                               9.6 UNSAFE    😨
dm-event.service                           9.5 UNSAFE    😨
emergency.service                          9.5 UNSAFE    😨
fail2ban.service                           9.6 UNSAFE    😨
getty@tty1.service                         9.6 UNSAFE    😨
ifup@enp0s3.service                        9.5 UNSAFE    😨
lvm2-lvmpolld.service                      9.5 UNSAFE    😨
lynis.service                              9.6 UNSAFE    😨
rc-local.service                           9.6 UNSAFE    😨
rescue.service                             9.5 UNSAFE    😨
rsyslog.service                            9.6 UNSAFE    😨
ssh.service                                9.6 UNSAFE    😨
systemd-ask-password-console.service       9.4 UNSAFE    😨
systemd-ask-password-wall.service          9.4 UNSAFE    😨
systemd-fsckd.service                      9.5 UNSAFE    😨
systemd-initctl.service                    9.4 UNSAFE    😨
systemd-journald.service                   4.3 OK        🙂
systemd-logind.service                     2.6 OK        🙂
systemd-networkd.service                   2.9 OK        🙂
systemd-timesyncd.service                  2.1 OK        🙂
systemd-udevd.service                      8.0 EXPOSED   😕
user@1000.service                          9.4 UNSAFE    😨
wpa_supplicant.service                     9.6 UNSAFE    😨
```

Analyse : le nombre de service en UNSAFE peut faire peur. Cependant, il faut prendre du recul sur l'outil, qui ne vérifie pas la configuration des services. Nous avons vérifié la configuration de tous les services en "UNSAFE" et "EXPOSED" et leur configuration nous satisfaisant, nous pouvons consiédrer les retours de la commande comme des faux-positifs.

If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]

Pourquoi ? Un 'core dump' est une copie (ou image) de la mémoire RAM d'un programme dont l'exécution a été intérrompue par le système en raison d'une erreur ou d'un quelconque problème. Ces fichiers sont destinés à aider les développeurs à débugger leurs programmes mais parfois ils peuvent contenir des informations sensibles. Il est donc plus sage de désactiver les 'core dump' si vous n'êtes pas développeur.

Comment ? Éditer le fichier `/etc/security/limits.conf` et ajouter/éditer la ligne :

```
* hard core 0
```

Cela limitera à 0 les core dumps pour tous les utilisateurs.

Ensuite, éditer le fichier `/etc/sysctl.conf` et ajouter la ligne :

```
fs.suid_dumpable = 0
```

Cela bloque les core dumps par les programmes en 'setuid'.

Puis, éditer le fichier `/etc/profile` et ajouter la ligne :

```
ulimit -S -c 0 > /dev/null 2>&1
```

Cela empechera la génération de core dumps pour tous les utilisateurs.

Configure maximum password age in /etc/login.defs [AUTH-9286]

Pourquoi ? Il est important que les utilisateurs changent fréquemment leurs mots de passes pour éviter qu'ils soient corrompus (leak de base de données par exemple) et puisse entrainer une compromission des informations (fichiers) auxquelles l'utilisateur a accès.

Comment ? Éditer la ligne `PASS_MAX_DAYS` dans le fichier `/etc/login.defs` avec le nombre de jours désiré.

Une semaine avant les 180 jours passés, si l'utilisateur n'a pas changé son mot de passe entre temps, alors il aura un message de WARNING à chaque connexion à sa session pour l'informer qu'il est temps de changer son mot de passe.

Configure minimum password age in /etc/login.defs [AUTH-9286]

Pourquoi ? Après la mise en place de la suggestion précédente (ci-dessus), l'utilisateur peut changer son mot de passe puis immédiatement revenir à l'ancien. Il faut donc bloquer ce comportement en empechant la réutilisation d'un ancien mot de passe jeune de X temps.

Comment ? Éditer la ligne `PASS_MIN_DAYS` dans le fichier `/etc/login.defs` avec le nombre de jours désiré.

Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

Pourquoi ? (se référer à la recommandation de l'ANSSI sur le umask (plus haut dans ce document) pour comprendre l'importance d'utiliser un umask fin)

Comment ? Éditer la ligne `UMASK` dans le fichier `/etc/login.defs` avec la valeur 0077.

Copy /etc/fail2ban/jail.conf to jail.local to prevent it being changed by updates. [DEB-0880]

Pourquoi ? Pour ne pas perdre la configuration du service fail2ban il est intéressant d'en faire une sauvegarde.

Comment ? Copier le fichier : Exécuter la commande : `cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`

Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]

Pourquoi ? Lorsque l'utilisateur change de mot de passe, il est important de s'assurer que ce mot de passe est sûr. Pour cela on peut installer un module PAM comme cracklib ou passwdqc.

Comment ? Installer le paquet libpam-cracklib : `apt install libpam-cracklib`

Determine if protocol 'dccp' is really needed on this system [NETW-3200]

Pourquoi ? Pour réduire la surface attaquable de notre système depuis le réseau, il est important de désactiver les protocoles qui ne nous servent pas/ne sont pas essentiels au bon fonctionnement du système.

Comment ? Créer un fichier `/etc/modprobe.d/dccp.conf` et y ajouter la ligne `install dccp /bin/true`.

Ensuite, éditer le fichier `/etc/modprobe.d/blacklist.conf` et y ajouter la ligne `blacklist dccp`.

Determine if protocol 'sctp' is really needed on this system [NETW-3200]

Pourquoi ? Pour réduire la surface attaquable de notre système depuis le réseau, il est important de désactiver les protocoles qui ne nous servent pas/ne sont pas essentiels au bon fonctionnement du système.

Comment ? Créer un fichier `/etc/modprobe.d/sctp.conf` et y ajouter la ligne `install sctp /bin/true`.

Ensuite, éditer le fichier `/etc/modprobe.d/blacklist.conf` et y ajouter la ligne `blacklist sctp`.

Determine if protocol 'rds' is really needed on this system [NETW-3200]

Pourquoi ? Pour réduire la surface attaquable de notre système depuis le réseau, il est important de désactiver les protocoles qui ne nous servent pas/ne sont pas essentiels au bon fonctionnement du système.

Comment ? Créer un fichier `/etc/modprobe.d/rds.conf` et y ajouter la ligne `install rds /bin/true`.

Ensuite, éditer le fichier `/etc/modprobe.d/blacklist.conf` et y ajouter la ligne `blacklist rds`.

Determine if protocol 'tipc' is really needed on this system [NETW-3200]

Pourquoi ? Pour réduire la surface attaquable de notre système depuis le réseau, il est important de désactiver les protocoles qui ne nous servent pas/ne sont pas essentiels au bon fonctionnement du système.

Comment ? Créer un fichier `/etc/modprobe.d/tipc.conf` et y ajouter la ligne `install tipc /bin/true`.

Ensuite, éditer le fichier `/etc/modprobe.d/blacklist.conf` et y ajouter la ligne `blacklist tipc`.

Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

Pourquoi ? Il est important d'informer les utilisateurs non autorisés qui essaient de se connecter au système des conséquences légales que ces connexions non désirées peuvent entrainer.

Comment ? Pour ajouter une bannière légale affichée lorsqu'une connexion à un compte utilisateur rate, éditez le fichier `/etc/issue` et ajoutez :

```
LEGAL DISCLAIMER :
Unauthorized use of this system is an offence under the Computer Misuse Act
 1990. By using this system you agree that your activity may be continuously
 monitored and that you will comply with the conditions of use.
```

Ce n'est qu'un exemple. Vous êtes libres d'y placer ce que vous voulez.

Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

Pourquoi ? Il est important d'informer les utilisateurs non autorisés qui essaient de se connecter au système des conséquences légales que ces connexions non désirées peuvent entrainer.

Comment ? Pour ajouter une bannière légale affichée lorsqu'une connexion à un compte utilisateur rate, éditez le fichier `/etc/issue.net` et ajoutez :

```
LEGAL DISCLAIMER :
Unauthorized use of this system is an offence under the Computer Misuse Act
 1990. By using this system you agree that your activity may be continuously
 monitored and that you will comply with the conditions of use.
```

Ce n'est qu'un exemple. Vous êtes libres d'y placer ce que vous voulez.

Enable process accounting [ACCT-9622]

Pourquoi ? Afin de savoir qui est responsable d'une faute (espace disque plein, comportement imprévu, ...) il est important de pouvoir suivre le comportement des processus.

Comment ? Installer le paquet 'acct' : `apt install acct`.

Note : Pour vérifier que le service tourne bien, utilisez la commande : `/etc/init.d/acct status`.

Note : Pour voir les temps d'activité par utilisateur, utilisez la commande : `ac -p`.

```
root@debian:~# ac -p
    clement                            65.61
    root                               14.58
    total       80.19
```

Note : Pour voir les processus ayant et les trier, utilisez la commande suivante :

```
root@debian:~# lastcomm | awk '{print $1}' | sort | uniq -c | sort -nr | head
    121 mandb
      6 sh
      5 systemctl
      4 systemd-detect-
      4 dpkg
      3 lastcomm
      2 who
      2 stty
      2 sort
      2 python3.9
```

Voici les outils disponibles :

```
      ac : statistiques sur les utilisateurs (utilise le fichier wtmp)
      accton : active/désactive le suivi des processus
      sa : fournit un résumé des informations de suivi (inclut les commandes
précédemment exécutées, les temps d'opération E/S, les temps CPU)
      lastcomm : affiche les commandes précédemment exécutées
```

Enable sysstat to collect accounting (no results) [ACCT-9626]

Pourquoi ? De même que la suggestion précédente avec les processus, il est intéressant d'avoir des informations sur le comportement du système.

Comment ? Installer le paquet 'sysstat' : `apt install sysstat`.

Voici les outils disponibles :

```
      sar : collecte et rapporte des informations sur l'activité du système
      iostat : rapporte l'utilisation du CPU et les statistiques d'E/S de disque
      mpstat : rapporte les statistiques générales et celles du processeur
      pidstat : rapporte les statistiques des processus Linux
      sadf : affiche les données collectées par sar
```

Ensuite, il faut activer 'sysstat'. Pour cela, éditer le fichier `/etc/default/sysstat` et éditer `ENABLED` à `"true"` :

```
ENABLED="true"
```

Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

Pourquoi ? Il est important de controller l'intégrité des fichiers importants/comportants des informations sensibles. Ce controlle peut s'effectuer automatiquement avec des programmes comme AIDE (Advanced Intrusion Detection Environment).

Comment ? Installer le paquet AIDE : `apt install aide`.
Il se configure à l'installation et tourne en tâche de fond.

Ensuite, il faut initiliser le programme : `/sbin/aideinit` (la commande peut prendre plusieurs minutes).

Et pour finir copier la base de données initialisée : `cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db`.

Tableau récapitulatif des règles

Terminée	Règle	Niveau	Intitulé	Principe
✔	R1	MIRE	Minimisation des services installés	Minimisation
✔	R2	-IRE	Minimisation de la configuration	Minimisation
☐	R3	--RE	Principe de moindre privilège	/
☐	R4	---E	Utilisation des fonctionnalités de contrôle d’accès	/
☐	R5	MIRE	Principe de défense en profondeur	/
☐	R6	--RE	Cloisonnement des services réseau	/
✔	R7	--RE	Journalisation de l’activité des services	Défense en profondeur
✔	R8	MIRE	Mises à jour régulières	Veille et maintenance
☐	R9	-IRE	Configuration matérielle	/
☐	R10	-IRE	Architecture 32 et 64 bits	/
☐	R11	---E	Directive de configuration de l’IOMMU	/
✔	R12	-IRE	Partitionnement type	Moindre privilège
✔	R13	--RE	Restrictions d’accès sur le dossier /boot	Défense en profondeur
☐	R14	-IRE	Installation de paquets réduite au strict nécessaire	/

Terminée	Règle	Niveau	Intitulé	Principe
☐	R15	MIRE	Choix des dépôts de paquets	/
☐	R16	--RE	Dépôts de paquets durcis	/
☐	R17	--RE	Mot de passe du chargeur de démarrage	/
✔	R18	MIRE	Robustesse du mot de passe administrateur	Minimisation
✔	R19	-IRE	Imputabilité des opérations d’administration	Défense en profondeur
☐	R20	--RE	Installation d’éléments secrets ou de confiance	/
✔	R21	-IRE	Durcissement et surveillance des services soumis à des flux arbitraires	Veille et maintenance
✔	R22	-IRE	Paramétrage des sysctl réseau	Défense en profondeur
✔	R23	-IRE	Paramétrage des sysctl système	Défense en profondeur
✔	R24	--RE	Désactivation du chargement des modules noyau	Défense en profondeur
✔	R25	--RE	Configuration sysctl du module Yama	Défense en profondeur
☐	R26	--RE	Désactivation des comptes utilisateurs inutilisés	/
☐	R27	-IRE	Désactivation des comptes de services	/
☐	R28	--RE	Unicité et exclusivité des comptes de services	/
☐	R29	--RE	Délai d’expiration de sessions utilisateurs	/
✔	R30	MIRE	Applications utilisant PAM	Moindre privilège
✔	R31	-IRE	Sécurisation des services réseau d’authentification PAM	Défense en profondeur
✔	R32	MIRE	Protection des mots de passe stockés	Défense en profondeur
☐	R33	-IRE	Sécurisation des accès aux bases utilisateurs distantes	/
☐	R34	-IRE	Séparation des comptes système et d’administrateur de l’annuaire	/
✔	R35	--RE	Valeur de umask	Moindre privilège
✔	R36	-IRE	Droits d’accès aux fichiers de contenu sensible	Moindre privilège
✔	R37	MIRE	Exécutables avec bits setuid et setgid	Moindre privilège
✔	R38	--RE	Exécutables setuid root	Moindre privilège
✔	R39	-IRE	Répertoires temporaires dédiés aux comptes	Moindre privilège

Terminée	Règle	Niveau	Intitulé	Principe
✔	R40	-IRE	Sticky bit et droits d’accès en écriture	Défense en profondeur
✔	R41	-IRE	Sécurisation des accès pour les sockets et pipes nommées	Défense en profondeur
✔	R42	MIRE	Services et démons résidents en mémoire	Minimisation
✔	R43	-IRE	Durcissement et configuration du service syslog	Défense en profondeur
✔	R44	-IRE	Cloisonnement du service syslog par chroot	Défense en profondeur
✔	R45	---E	Cloisonnement du service syslog par conteneur	Défense en profondeur
✔	R46	-IRE	Journaux d’activité de service	Veille et maintenance
✔	R47	-IRE	Partition dédiée pour les journaux	Veille et maintenance
☐	R48	-IRE	Configuration du service local de messagerie	/
☐	R49	-IRE	Alias de messagerie des comptes de service	/
✔	R50	--RE	Journalisation de l’activité par auditd	Veille et maintenance
☐	R51	---E	Scellement et intégrité des fichiers	/
☐	R52	---E	Protection de la base de données des scellés	/
☐	R53	--RE	Restriction des accès des services déployés	/
☐	R54	--RE	Durcissement des composants de virtualisation	/
☐	R55	-IRE	Cage chroot et privilèges d’accès du service cloisonné	/
☐	R56	-IRE	Activation et utilisation de chroot par un service	/
✔	R57	-IRE	Groupe dédié à l’usage de sudo	Défense en profondeur
✔	R58	-IRE	Directives de configuration sudo	Défense en profondeur
✔	R59	MIRE	Authentification des utilisateurs exécutant sudo.	Défense en profondeur
✔	R60	-IRE	Privilèges des utilisateurs cibles pour une commande sudo	Défense en profondeur
✔	R61	--RE	Limitation du nombre de commandes nécessitant l’option EXEC	Défense en profondeur

Terminée	Règle	Niveau	Intitulé	Principe
✔	R62	-IRE	Du bon usage de la négation dans une spécification sudo.	Défense en profondeur
✔	R63	-IRE	Arguments explicites dans les spécifications sudo	Défense en profondeur
✔	R64	-IRE	Du bon usage de sudoedit	Défense en profondeur
✔	R65	---E	Activation des profils de sécurité AppArmor	Défense en profondeur
☐	R66	---E	Activation de SELinux avec la politique targeted	/
☐	R67	---E	Paramétrage des booléens SELinux	/
☐	R68	---E	Désinstallation des outils de débogage de politique SELinux	/
☐	R69	---E	Confinement des utilisateurs interactifs non privilégiés	/

Anecdote : historique des instantanés