Documentation technique

Durcissement Linux en environnement isolé

Application des recommandations ANSSI BP-028 sur Ubuntu Server

Type de document	Compte rendu technique
Environnement	Ubuntu Server sous Hyper-V
Contrainte principale	Machine isolée du réseau (Air-Gap)
Référentiel	Guide de configuration GNU/Linux ANSSI BP-028

Synthèse exécutive

Le durcissement vise à réduire la surface d'attaque locale d'un serveur critique isolé. Les mesures portent sur le démarrage, le noyau, les privilèges, les permissions, les comptes locaux, les services, le maintien en condition de sécurité et la validation par tests de robustesse.

1. Contexte et objectif

Ce document présente la démarche de durcissement d'un serveur Ubuntu Server déployé sous Hyper-V, dans un environnement totalement isolé du réseau. L'intervention s'inscrit dans une logique de sécurisation locale renforcée, en appliquant autant que possible les recommandations du guide ANSSI BP-028.

La machine étudiée ne dispose pas d'accès SSH, n'est pas connectée au réseau de l'entreprise et repose sur un compte administrateur local unique. Cette contrainte impose une approche pragmatique : certaines mesures réseau ou centralisées sont inapplicables, tandis que les protections locales sont renforcées en profondeur.

2. Sécurisation du démarrage GRUB

Le premier niveau de protection consiste à verrouiller le chargeur de démarrage afin d'empêcher toute modification non autorisée des paramètres du noyau depuis la console de prédémarrage.

Un mot de passe GRUB chiffré a été généré, puis intégré dans le fichier de configuration personnalisé. Les options du noyau ont également été renforcées pour désactiver IPv6 dès le démarrage et activer plusieurs protections mémoire.

```
grub-mkpasswd-pbkdf2 > /tmp/grub_pass.txt
# Modification de /etc/grub.d/40_custom
# Ajout de ipv6.disable=1 iommu=force page_poison=on pti=on slab_nomerge=yes
update-grub
rm /tmp/grub_pass.txt
```

Figure 1 - Déclaration du super-utilisateur GRUB et ajout du condensé PBKDF2.

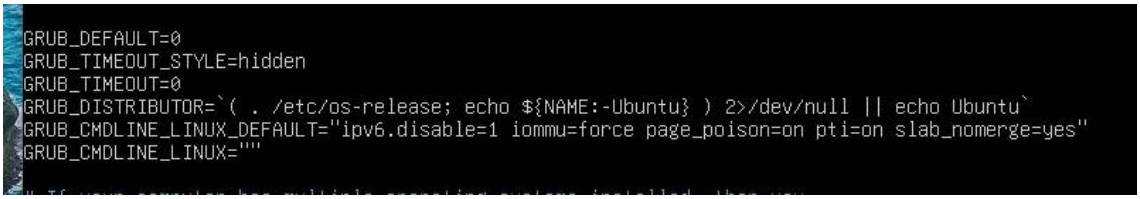

Figure 2 - Options de démarrage renforcées dans la configuration GRUB.

3. Durcissement du noyau avec sysctl

Le fichier /etc/sysctl.conf a été utilisé pour appliquer des restrictions persistantes au niveau du noyau Linux. L'objectif est de limiter les capacités d'observation, de réduire les vecteurs d'attaque réseau locaux et d'empêcher le chargement de modules supplémentaires après durcissement.

Les paramètres appliqués couvrent notamment la désactivation IPv6, la restriction de dmesg, la protection des pointeurs mémoire, le contrôle de ptrace, la protection des liens symboliques et physiques, ainsi que la protection contre les redirections ICMP et le spoofing.

```
kernel.modules_disabled = 1
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
kernel.dmesg_restrict = 1
kernel.kptr_restrict = 2
kernel.yama.ptrace_scope = 1
fs.protected_symlinks = 1
fs.protected_hardlinks = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.rp_filter = 1
sysctl -p
```

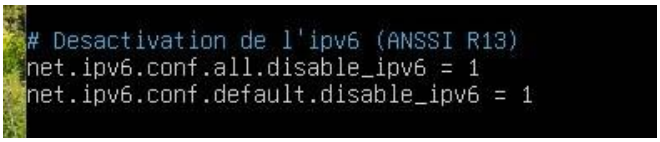

Figure 3 - Désactivation d IPv6 au niveau sysctl.

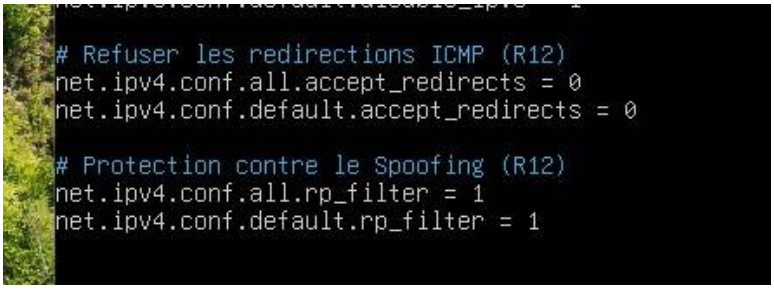

Figure 4 - Protection contre les redirections ICMP et le spoofing.

4. Contrôle d'accès et durcissement de sudo

Le principe du moindre privilège a été appliqué en limitant l'usage de sudo à un groupe dédié. Les directives globales ont été renforcées afin de réduire les risques liés aux shells interactifs, aux variables d'environnement et à l'exécution de sous-processus.

```
groupadd sudogrp
usermod -aG sudogrp mbappe
visudo
Defaults noexec, requiretty, use_pty, umask=0027
Defaults ignore_dot, env_reset
```

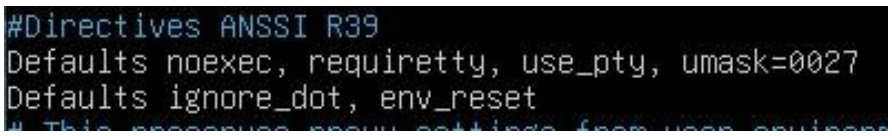

Figure 5 - Directives sudo renforcées conformément au principe de moindre privilège.

5. Synthèse des mesures locales appliquées

Domaine	Mesure appliquée	Recommandation	Effet recherché
Démarrage	Mot de passe GRUB et options noyau	R5, R7, R8, R13	Empêcher la modification du boot et renforcer la mémoire
Noyau	Paramètres sysctl restrictifs	R9 à R14	Réduire la surface d attaque

			système et réseau
Privilèges	Groupe sudo dédié et directives strictes	R38, R39	Limiter les actions administratives
Fichiers	Sticky bit, /boot en 700, umask 0077	R29, R36, R54	Protéger les fichiers sensibles et temporaires
Comptes	Root verrouillé, compte sync neutralisé	R33, R34	Fermer les accès locaux non nécessaires
Services	Désactivation des démons inutiles	R62	Réduire les processus exposés
MCS	Mise à jour manuelle via ISO	R61	Maintenir le système sans connexion réseau

6. Système de fichiers et permissions

Les permissions locales ont été renforcées afin d'empêcher la lecture ou la suppression non autorisée de fichiers. Le sticky bit a été vérifié sur /tmp, l'accès à /boot a été restreint et un umask strict a été appliqué pour les nouveaux fichiers.

Figure 6 - Restriction des droits sur /boot.

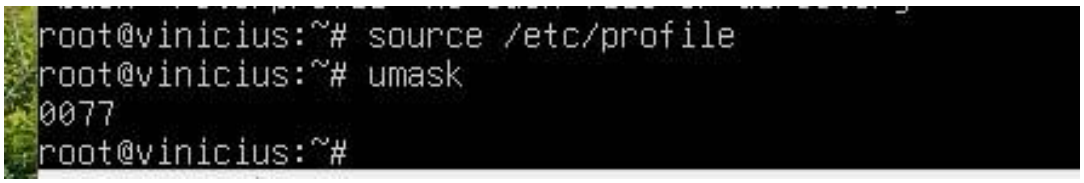

Figure 7 - Application et vérification du masque umask 0077.

7. Verrouillage des comptes locaux

Les comptes capables d'ouvrir une session interactive ont été inventoriés. Le compte root a été verrouillé pour empêcher toute connexion directe, et le compte système sync a été neutralisé en lui retirant son shell interactif.

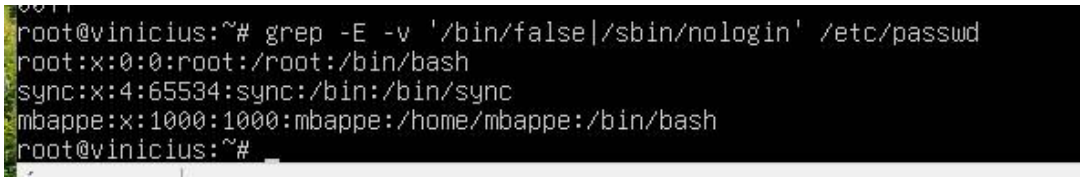

Figure 8 - Inventaire des comptes disposant d un shell interactif.

8. Gestion des limites liées à l Air-Gap

L'isolement complet du serveur rend certaines recommandations inapplicables : centralisation SYSLOG, authentification Kerberos ou Active Directory, supervision, EDR, mise à jour automatique et installation classique d'auditd. Ces points ont été documentés comme limitations techniques et compensés par des mesures locales.

9. Audit des droits SUID et SGID

Les exécutables disposant de droits spéciaux ont été audités. Les droits nécessaires aux composants vitaux ont été conservés, tandis que les bits SUID de commandes interactives inutiles ont été retirés afin de réduire les possibilités d'escalade locale.

```
find / -type f -perm /6000 -ls 2>/dev/null
chmod u-s /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp
```

Figure 9 - Liste des fichiers SUID/SGID recensés sur le système.

Figure 10 - Retrait du bit SUID sur les commandes non nécessaires.

10. Protection cryptographique et confinement

La politique de hachage des mots de passe a été vérifiée dans PAM afin d'utiliser un algorithme robuste tel que yescrypt. Le confinement AppArmor a également été contrôlé en interrogeant directement le noyau, confirmant l'activation du module de contrôle d'accès obligatoire.

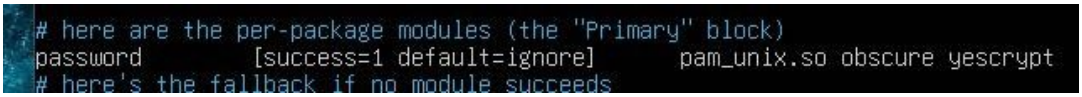

Figure 11 - Configuration PAM utilisant yescrypt.

Figure 12 - Vérification de l activation d AppArmor.

11. Nettoyage du système et services inutiles

Les services actifs ont été listés avec systemctl. Les démons inutiles dans ce contexte de machine virtuelle isolée ont été désactivés : ModemManager, fwupd, upower, multipathd, unattended-upgrades et systemd-timesyncd.

```
systemctl list-units --type=service --state=running
systemctl disable --now ModemManager unattended-upgrades systemd-timesyncd fwupd upower multipathd
```

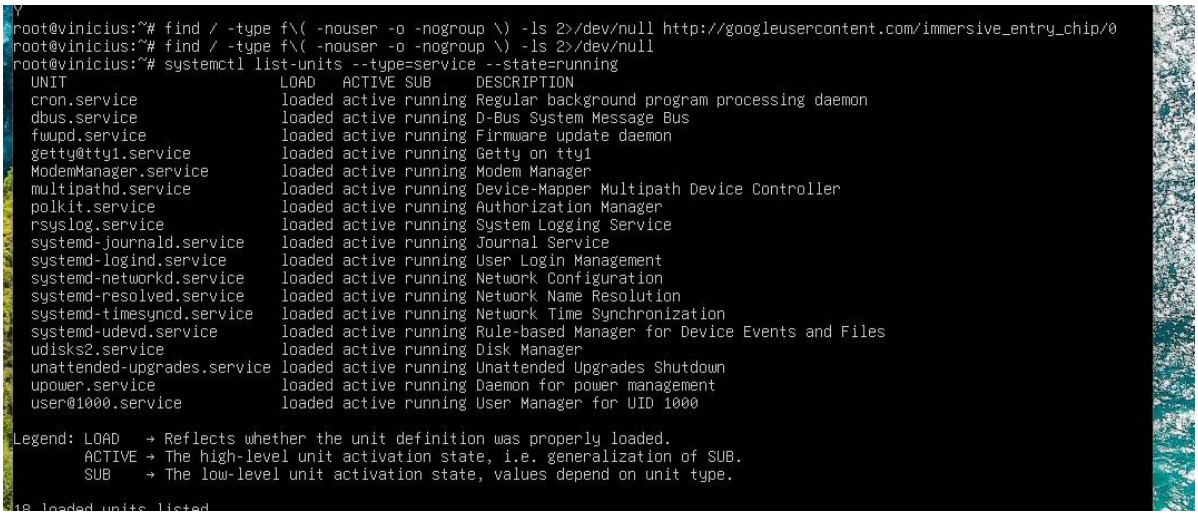

Figure 13 - Inventaire des services actifs.

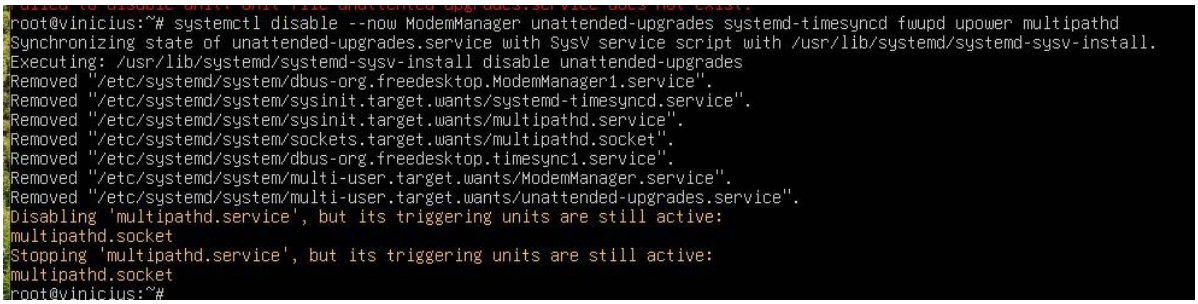

Figure 14 - Désactivation groupée des services superflus.

12. Maintien en Condition de Sécurité en Air-Gap

L'absence d'accès réseau impose une procédure de mise à jour manuelle. Le maintien en condition de sécurité repose sur le téléchargement mensuel d'une image ISO de paquets depuis une machine connectée, son montage dans Hyper-V, puis sa déclaration comme source locale de confiance via apt-cdrom.

```
sudo mount /dev/cdrom /media/cdrom
sudo apt-cdrom -m -d /media/cdrom add
sudo apt update
```

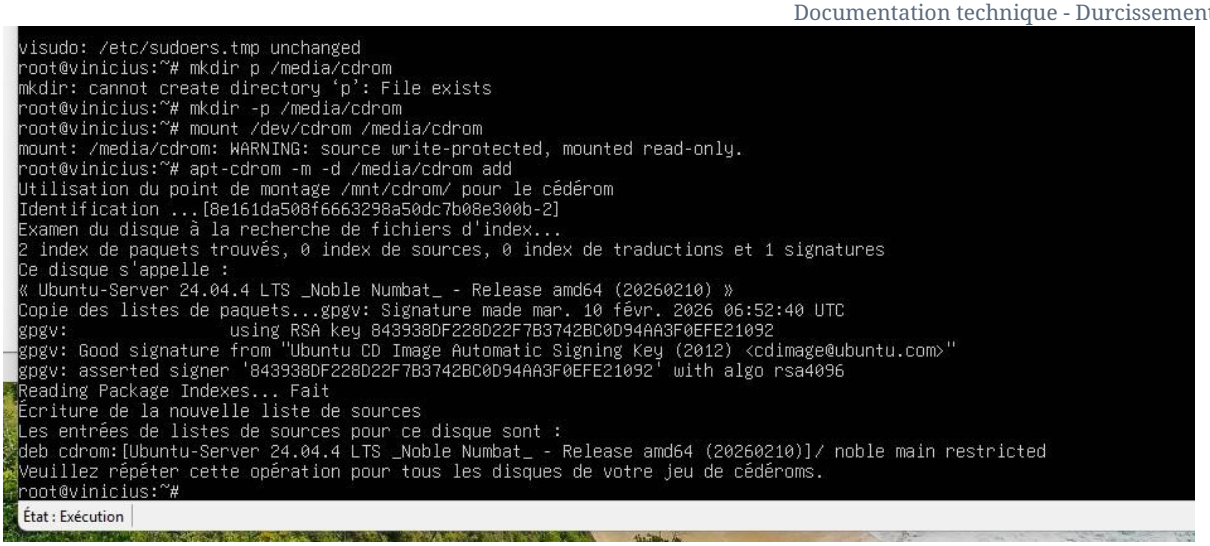

Figure 15 - Ajout du support ISO comme source APT locale.

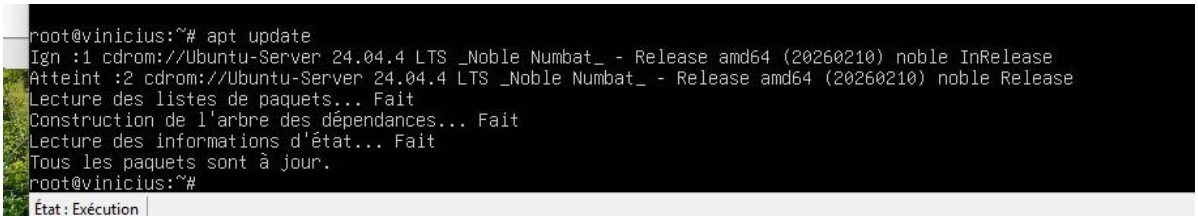

Figure 16 - Mise à jour depuis le dépôt local monté.

13. Validation de l audit

Les tests de robustesse ont confirmé l'efficacité des protections : absence d'IPv6, rejet des connexions directes au compte root, arrêt des services inutiles et blocage d'opérations administratives par la directive sudo noexec.

Ce dernier point illustre la puissance du durcissement : la restriction empêche l'exécution de sous-processus furtifs, mais peut aussi bloquer des opérations de maintenance légitimes si elle n'est pas accompagnée d'une procédure d'administration dédiée.

Figure 17 - Validation de la désactivation IPv6 avec ip a.

14. Incident majeur : verrouillage de l administrateur

Le durcissement extrême a provoqué un cas d'école : la perte d'accès administratif légitime. Les tentatives de correction via sudo -i, visudo, modification GRUB, puis Live CD ont été arrêtées par les différentes couches de protection : noexec, mot de passe GRUB, Secure Boot et restrictions Hyper-V.

Cet incident démontre qu'un durcissement efficace doit toujours être accompagné d'une stratégie de réversibilité : compte de secours, sauvegarde de configuration, snapshot Hyper-V, procédure de restauration documentée et validation progressive des règles.

Figure 18 - Blocage des commandes administratives par la directive sudo noexec.

15. Bilan final

Le projet aboutit à un serveur localement très fortement durci, mais met en évidence un équilibre fondamental : confidentialité et intégrité ont été maximisées au détriment de la disponibilité. Dans un environnement Air-Gap critique, ce choix peut être cohérent, mais il doit rester maîtrisé par des mécanismes de récupération prévus avant l'application des règles les plus restrictives.

Recommandation

Avant toute généralisation, appliquer les mesures par lots, réaliser un snapshot avant chaque phase, conserver un compte de secours documenté et tester les procédures de reprise. Le durcissement doit être sécurisé, mais aussi administrable.