Durcissement Debian Cheat Sheet

by Varg via cheatography.com/133204/cs/27134/

Partitions

Bien identifier les partitions à isoler tel que : /, /boot, /home, /var

/etc/fstab	Fichier de configuration des partitions
luks	(Linux Unified Key Setup) : standard de chiffrement
`fdisk`	Permet de manipuler les partitions
`cryptsetup`	Permet de manipuler des volumes cryptographiques
`mount` et `unmont`	Permet de monter et démonter une partition

BIOS/UEFI & Grub

Mettre à jour le bios et lui mettre un mot de passe

Contrôler les périphériques de démarrage et la séquence de démarrage

Grub permet d'accéder en root au système, il est donc nécessaire de lui mettre un mot de passe

`grub-mkpasswd-pbkdf2`	Génère un hash du mot passe grub

Logiciels sécurités

netfilter	Parefeu Linux
fail2ban	Framework de prévention contre les intrusions
clamav	Antivirus Linux
ssh	Accès sécurisé en lignes de commandes à distance

Gestion des évènements

syslog (dernière version : rsyslog)	Protocole et format de références des évènements
/var/log	Répertoire de stockage des jounaux
journalctl	Permet de consulter les journaux systemd
auditd	Permet de surveiller les actions des utilisateurs

Sauvegardes

Toujours avoir une copie des fichiers sur un support différent de la source et idéalement dans un autre lieu

Réduire la taille d'un fichier (grâce à la compression) permet de limiter le taux d'occupation des disques

rsync	Logiciel de synchronisation de fichiers

Nettoyage OS

`systemctl`	Contrôle le système systemd et le gestionnaire de service
`lsmod`	Liste les statuts des modules noyau
`modprobe`	Permet de manipuler les modules chargeables
`sysctl`	Permet de modifier la configuration de certains modules
/etc/issue & /etc/issue.net	Contient la bannière affichée lors d'une connexion locale & distante

Paquets

`apt-get install` *`paquet`*	Installer un *paquet*
`apt-get update` & `apt-get upgrade`	Met à jour la liste des paquets disponibles & Installe les mise à jour disponibles de tous les paquets

Utilisateurs

`sudo`	Permet d'exécuter une action avec l'identité d'un autre utilisateur
`gpasswd`	Permet d'administrer les groupes d'utilisateurs
/etc/sudoers	Fichier de configuration des utilisateurs sudo
/etc/login.defs	Fichier de configuration de la suite des mots de passe cachés « shadow password »
/etc/shadow	Contient une version hashée des mots de passe des utilisateurs
/etc/passwd	Base de données textuelle d'informations sur les utilisateurs qui peuvent se connecter au système
`chown`	Changer l'utilisateur ou le groupe
`chmod`	Changer les droits d'un fichier ou répertoire
`usermod`	Modifier un compte utilisateur
`chroot`	Permet de modifier la racine dans le contexte d'exécution
PAM	Permet de configurer des méthodes pour authentifier les utilisateurs

By **Varg**
cheatography.com/varg/

Published 17th March, 2021.
Last updated 18th March, 2021.