Projet Labo SSI

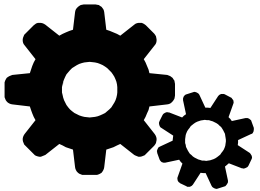
Mise en place d'une station blanche

FEUGERE Thibault

Constat

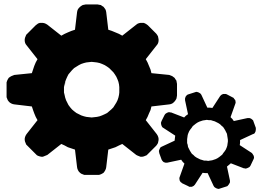
Qu’est-ce qu’une station blanche ?

Objectifs



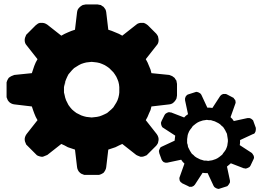
1. Recherches station blanche
2. Recherches antivirus
3. Choix OS
4. Hardening
5. Documentation
6. Prise de recul

Menaces



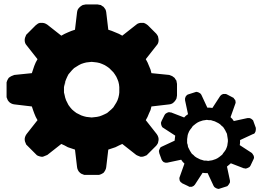
- Utilisateur légitime
- Utilisateur non autorisé
- Attaquant avec droits administrateurs

Système d’exploitation



- Q4OS
- RAM: 128 MB
- CPU: 300 MHz
- Espace de stockage : 5 GB
- Chiffré

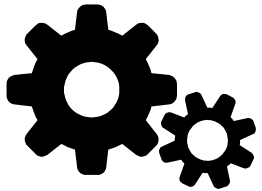
Pare-feu



- UFW - Politique restrictive

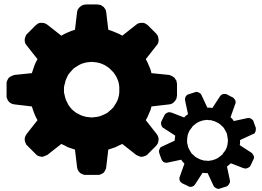
- DNS
- HTTP / HTTPS

Installation



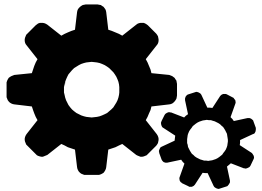
- OVA
- OS debian avec *install-all.sh*

Scan



- ClamAV (+ cron)
- VirusTotal

Update



- Mise à jour OS
- Scan debsecan
- Mise à jour Clamav
- Lynis

Hardening

[Lynis 3.0.3 Results]-

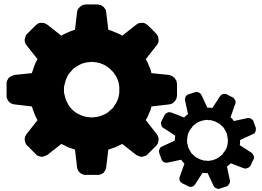
  Warnings (3):

  ! grpck binary found errors in one or more group files [AUTH-9216]
      https://cisofy.com/lynis/controls/AUTH-9216/

  ! No AIDE database was found, needed for AIDE functionality [FINT-4316]
      https://cisofy.com/lynis/controls/FINT-4316/

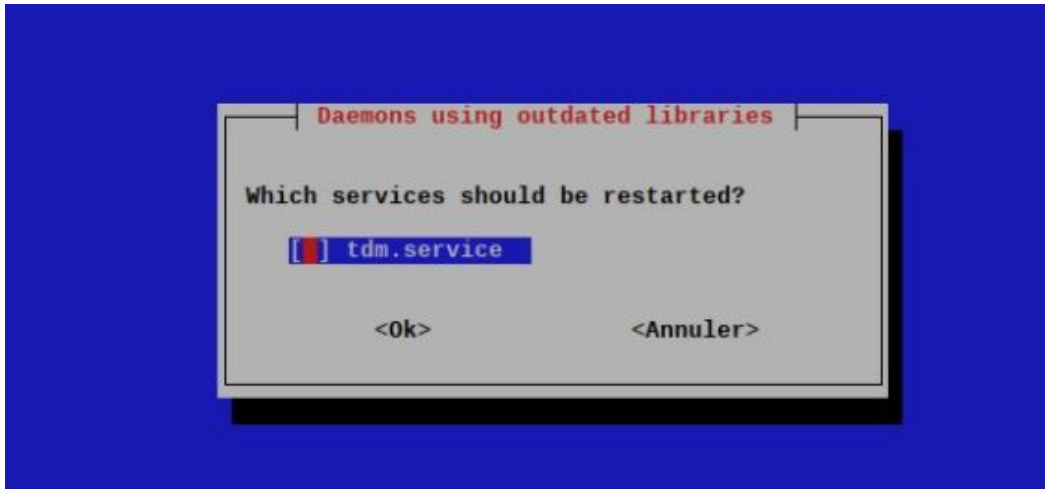
  Suggestions (35):
  ----
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/

Outils

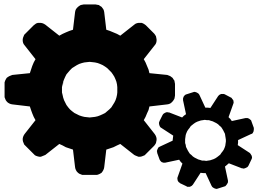


- Debsums
- Debsecan
- Debian-goodies
- Needrestart

Outils

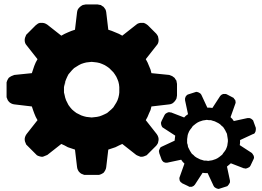

Daemons using outdated libraries
Which services should be restarted?
[ ] tdm.service
<Ok>
<Annuler>

Debsecan



- debsecan --suite buster --only-fixed
- apt install $(debsecan --suite buster --only-fixed --format packages)

Problèmes



- Plusieurs petits problèmes
- Très peu de documentation

Démonstration

Merci !

https://gitlab.com/thibaultfeugere/station-blanche

FEUGERE Thibault