Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Hes·so VALAIS WALLIS
School of Management

IT Infrastructure Hardening Automation

Etudiant : Thomas Luyet
Professeur : Xavier Barmaz

Résumé

1. Etat de l'art sur la base du **Hardening** et des solutions permettant son **automatisation**.
2. **Analyse comparative des solutions disponibles** Open Source et gratuites pour OS Windows et Linux.
3. **Développement** d'une solution personnalisée.

Introduction

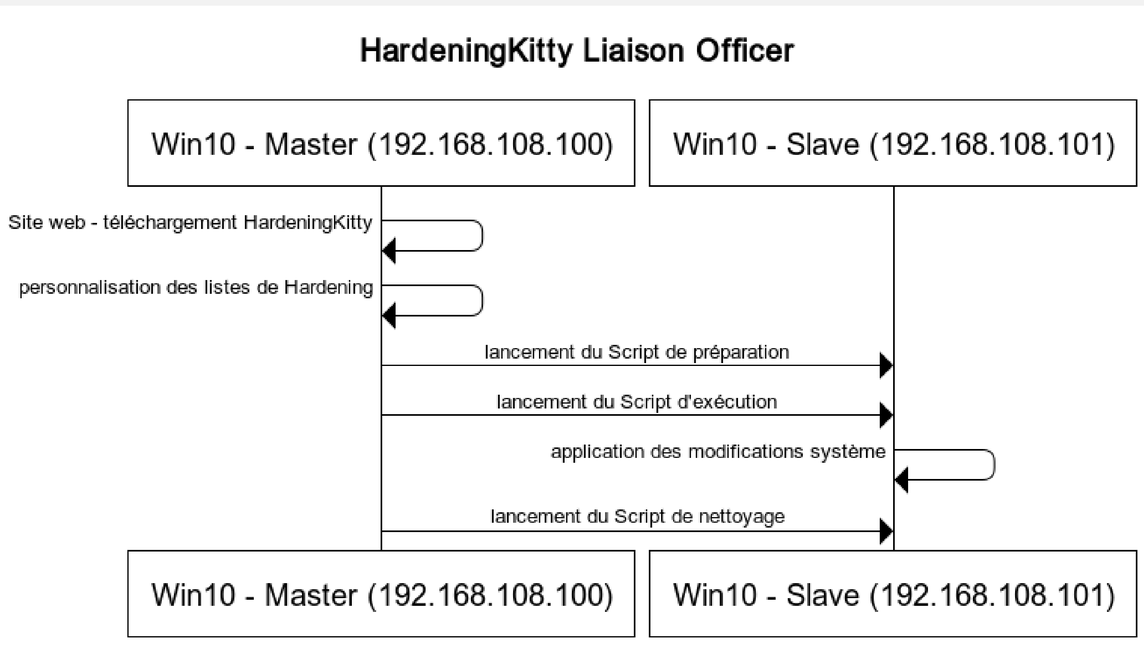
- Avec l'augmentation des cyber-attaques, le renforcement des infrastructures IT s'impose.
- Le **Hardening** permet ce **renforcement en comblant les failles** présentes nativement dans les systèmes.
- La solution réside dans l'application de **recommandations,** telles que : **CIS, STIG, ANSSI, SiSyPHus** provenant de différents pays et organisations. Ces «bonnes pratiques» sont présentes sous forme de documents contenant l'ensemble des actions à mener pour durcir la sécurité de son infrastructure.
- Notre objectif est de **trouver une solution**, pour une PME, qui soit **Open Source et gratuite** permettant d'**automatiser le durcissement des infrastructures** sur une machine distance et sans utiliser d'agent.

Méthodes

- Tests en laboratoire virtuel de plusieurs solutions.
- Constat : la solution **HardeningKitty** est la meilleure disponible. Elle permet la possibilité de réaliser des **Scans**, du **Hardening**, des **Audits** et des **Backups** mais n'offre pas la possibilité de travailler sur une machine distante et ne dispose d'aucun menu.
- Création de **HardeningKitty Liaison Officer** composé de **Scripts** permettant l'exécution de HardeningKitty sur une machine distante au moyen d'un menu.
- Utilisation des **protocoles SCP et SSH** pour le transfert de fichiers et la connexion à une machine distante. **Authentification SSH par clés**.

Résultats

- Aucune solution trouvée ne correspond à l'objectif fixé dans notre recherche.
- **Les solutions Open Source et gratuites sont rares** et ne couvrent qu'une famille de système d'exploitation, soit Windows soit Linux.
- Il est **possible de combiner des solutions existantes** pour obtenir de meilleures performances.
- Utiliser une solution disponible comme moteur de base et **développer sa propre solution apportant des fonctionnalités supplémentaires** permet d'atteindre l'objectif pour les systèmes d'exploitation Windows.



Outils

Windows 10 · OpenSSH · VirtualBox

Conclusions

- Notre infrastructure numérique doit être considérée comme une forteresse. Plus notre infrastructure est renforcée moins nous sommes vulnérables aux attaques. C'est pourquoi, le Hardening est essentiel dans une architecture de cybersécurité.
- La solution miracle, All-in-One, Open Source et gratuite, n'existe pas. En revanche, il est possible de trouver des solutions de qualité et de les adapter à son environnement afin d'automatiser le Hardening.

HES-SO Valais-Wallis • rte de la Plaine 2 • CP 80 • 3960 Sierre
+41 58 606 93 11 • info@hevs.ch • www.hevs.ch/ig

Contact and more informations:
http://www.hevs.ch/ig