Introduction

Le durcissement (ou *hardening*) fait partie du processus de sécurisation d'une infrastructure qu'elle soit virtuelle ou physique et se fait à plusieurs niveaux. Il y a la protection physique, sous-entendue accès aux locaux, baies et serveurs, et le niveau logique qui correspond aux configurations des couches systèmes et applicatives.

En France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est responsable de l'édition des règles de bonnes pratiques pour les OIV (Operateur d'Importance Vitale) comme les particuliers.

En juillet 2016, l'ANSII a livré un guide des bonnes pratiques (de sécurité) concernant la version 5.5 de VMware vSphere. Il comprend 46 recommandations sur 10 sujets. Ce guide est disponible ici (http://www.ssi.gouv.fr/uploads/2016/07/np_vmwareesx_notetech_v1.pdf). Maintenant n'oublions pas qu'un hyperviseur s'appuie sur un matériel basé sur des microprocesseurs de type x86 (x86, x86_64) dont le guide de bonne pratique se trouve là (http://www.ssi.gouv.fr/uploads/2015/03/NP_ConfigMateriel.pdf), qui lui date de 2015.

VMware publie son guide de mesures de sécurité qui inclut la recommandation, mais aussi la mise en place et le contrôle du correctif pour les paramètres concernés. Le guide pour la version 6.5 est disponible depuis le 17 avril. Il se présente sous la forme de tableaux MS Excel (https://www.vmware.com/co).

Guideline ID	Catégories (patch, configuration...)
Risk Profile	Niveaux de criticité
Description	Description
Vulnerability Discussion	Explication concernant la vulnérabilité
Configuration Parameter	Paramètre à configurer
Desired Value	Valeur voulue
Default Value	Valeur par défaut
Is desired value the default?	Est-ce la valeur par défaut ?
Action Type	Type d'action
Assessment using Web Client	Vérification via le client web
Negative Functional Impact	Régression fonctionnelle
Remediation using Web Client	Correction via le client web
vSphere API	API (interface de programmation) vSphere
ESXi Shell Command Assessment	Vérification via les lignes de commandes
ESXi Shell Command Remediation	Correction via les lignes de commandes de l'hyperviseur
vCLI Command Assessment	Vérification via les lignes de commandes de l'appliance vMA
vCLI Command Remediation	Correction via les lignes de commandes de la vMA
PowerCLI Command Assessment	Vérification via Powershell
PowerCLI Command Remediation	Correction via Powershell
Able to set using Host Profile	S'il est possible de le configurer via les profils d'hôtes
Reference	Référence dans la documentation VMware et dans les blogs VMware

Ce document contient 76 options de durcissement permettant d'augmenter le niveau sécurisation de l'infrastructure. Certaines options sont déjà des habitudes telles que le retrait des lecteurs de CD-ROM et de disquette, tandis que d'autres le sont beaucoup moins tel que la désactivation du copier/coller via la console de la machine virtuelle et l'accès distant (poste utilisateur).

De la même manière, les bonnes pratiques définies par ces documents et d'autres, sont des règles de conduite, il faut donc les tester et les valider dans vos environnements.

Il existe quelques outils pour auditer et renforcer une infrastructure vSphere tels que :

- Les STIG (*Security Technical Implementation Guide*).
- L'appliance Runecast.

Parallèlement à ces documents, avec la sortie de vSphere 6.5, VMware a mis à jour son guide de sécurité (https://pubs.vmware.com/vsphere-65/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-65-security-guide.pdf). Il contient les explications sur la configuration et les Best Practice pour les périmètres touchés par un besoin sécuritaire (accès, réseaux...).

Nous allons couvrir plus spécifiquement dans ce chapitre

- Le Secure boot.
- Le chiffrement (certificats, vMotion, VM).
- Les gestions des accès au niveau d'une infrastructure VMware (Active Directory, vCenter SSO).