1 SECURISER SES SYSTEMES

Les bonnes pratiques de configuration permettent d'éviter un certain nombre d'actions malveillantes sur les systèmes et de protéger les données sensibles, tels que les données de ***pen testing*** de vos futurs clients !

Un ensemble d'actions peuvent permettre d'assurer un minimum la sécurisation de vos systèmes. C'est dans cette optique que nous allons discuter du hardening système.

1.1. Qu'est-ce que le Hardening Système ?

Le Hardening Système vise à fortifier une machine, un serveur, un poste client, dans l'optique d'en augmenter le niveau de sécurité. Le but premier du hardening est de réduire le nombre d'objets (utilisateurs, bibliothèques, applications, etc.) présents sur le système, en ne conservant que ceux qui sont nécessaires au bon fonctionnement du serveur et du service rendu par ce dernier.

Un certain nombre de guides sont disponibles, en générale, rédigés par des agences de sécurités influentes. Ils visent à établir un socle « sain » en atteignant des niveaux de sécurité plus ou moins élevés sur certains aspects du système. Il est possible de trouver sur internet des guides de Hardening fournis par exemple par la NSA, le CIS, le DISA. Pour une même technologie, il existe quelques différences de prérequis entre ces différents guides pour être « compliant ».

https://public.cyber.mil/stigs/

Les guides de hardening STIGs sont fournis par le DISA dans le but de fixer des niveaux de sécurité à observer pour le DoD Américain (U.S. Department of Defense). Un STIG est donc une sorte de "checklist". Chaque vérification (check) est identifiée par un ID et associée à un niveau de criticité (CAT.1 le plus critique, CAT.3 le moins critique).

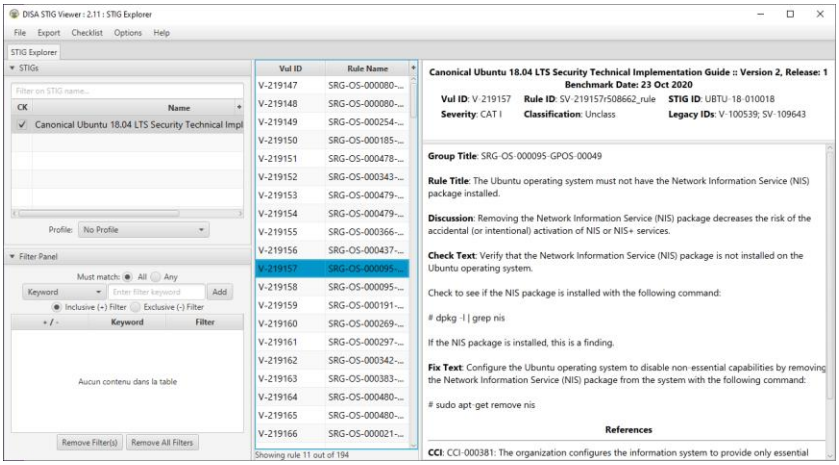
En termes d'implémentation, il ne s'agit pas d'appliquer l'ensemble des correctifs fournis par un STIG. Cela est en général incompatible avec la façon dont fonctionne de manière spécifique un système au sein d'un environnement autre que celui du DoD.

L'idée ici est donc de reprendre certains points clés, qui sont intéressants et qui concernent des éléments que l'on peut modifier sur le système sans impacter l'expérience utilisateur. Pour ce faire, il est intéressant de se focaliser sur les niveaux de criticités I (fort) et II (moyen) et de cibler les éléments qui nous intéressent.

1.2. Exercice

1. Sur le site des du DISA, recherchez et téléchargez les STIG pour un système Windows 10, Windows Server 2016 et Ubuntu 18.04 LTS.

2. Installez et utilisez le STIG Viewer pour visualiser le contenu de vos découvertes.



2 SECURISATION KALI LINUX

Comme vous pourrez le constater, tous les systèmes ne sont pas répertoriez et il faut parfois rechercher les manuels de bonnes pratiques sur le Web. Dans ce laboratoire, nous allons reprendre la sécurisation d'un nouvel environnement Kali Linux. Pour cela, je vous invite à télécharger le document officiel **Kali Linux Revealed** mis en ligne sur la page HELMo Learn ou téléchargeable sur le site https://www.kali.org/download-kali-linux-revealed-book/

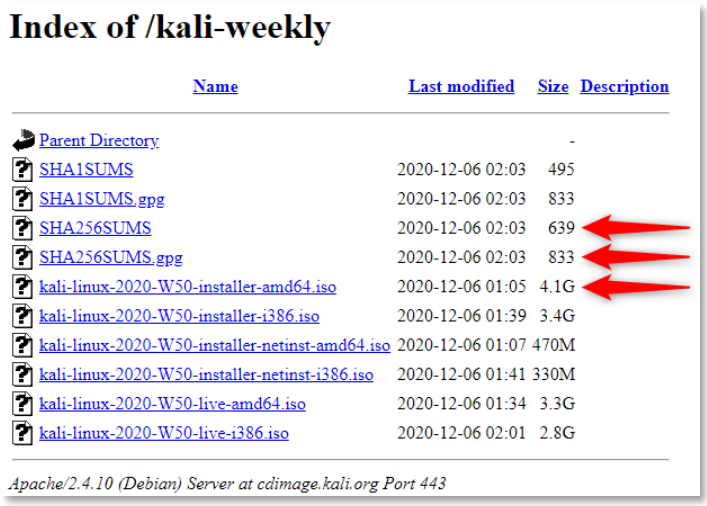
2.1. Exercice

1. Lisez le chapitre **7 - Securing and Monitoring Kali Linux**

2. Au point **7.1. Defining a Security Policy**, répondez à ces trois questions :

   - **Qu'est-ce que vous essayez de protéger ?**
   - **Contre quoi essayez-vous de vous protéger ?**
   - **De plus, contre qui essayez-vous de vous protéger ?**

3. Procurez-vous l'image ISO Kali Linux 64 bits dernière version en ligne sur la page https://www.kali.org/downloads/ et placez cette image dans un dossier **Kali_image**



4. Renseignez les étapes suivies pour validez l'authenticité de votre téléchargement. Vous pouvez vous aider du labo 6 et des instructions reprises sous la rubrique **Download Kali Linux Images Securely** sur https://www.kali.org/downloads/

   Si vous avez suivi scrupuleusement les étapes du labo 6, vous devriez obtenir ceci à la vérification de la signature des SHA256SUMS :

```
C:\Users\MANGONChristophe\Downloads\Kali_image>gpg --verify SHA256SUMS.gpg SHA256SUMS
gpg: Signature made Sun Dec  6 03:03:33 2020
gpg:                using RSA key 44C6513A8E4FB3D30875F758ED444FF07D8D0BF6
gpg: Good signature from "Kali Linux Repository <devel@kali.org>" [full]
```

5. Une fois la signature de votre fichier SHA256SUMS validée, vérifiez l'intégrité de votre fichier image à l'aide de l'outil GtkHash

6. A partir de ces éléments, nous allons réaliser une nouvelle installation Kali Linux sur un disque totalement crypté en suivant la procédure **4.2.2. Installation on a Fully Encrypted File System** sur notre environnement VMware Workstation (sur Windows) ou Fusion (sur MacOS) en suivant les recommandations du chapitre **2.2.2. In a Virtual Machine** (page 36).
   NE PAS UTILISER LA VM Kali 2020 utilisée jusqu'à maintenant pour ce labo !
   Cette VM doit rester opérationnelle pour vos examens de janvier !

7. Votre nouvelle VM devra être configurée avec l'interface eth0 en mode NAT sur l'adresse IP 192.168.254.10/24, sa default route 192.168.254.2 et ses DNS 9.9.9.9 et 1.1.1.1.

8. Réalisez une mise à jour de votre nouvelle VM (`apt-get update && apt-get upgrade`)

9. Installez les VMware Tools

10. A partir de votre sauvegarde réalisée dans le labo 7, resaurez les éléments nécessaires pour retrouver un environnement opérationnel (SSH, utilisateurs, home directories, groups, clés GPG, etc.)

11. Créez et testez une connexion client SSH sur PuTTY vers votre nouvelle VM.

12. Installez votre script de sauvegarde comme réalisé dans le labo 6, mais en renommant votre disque de partage avec votre host.

13. Sécurisez votre système en suivant les recommandations du chapitre **7** - **Securing and Monitoring Kali Linux**