SOS
Sécurité des systèmes

EXAMEN PRATIQUE

Forme :

- Ce lab doit être réalisé **par groupe de deux maximum**
- Ce lab contient une démarche technique qui consiste à effectuer plusieurs configurations sur un système Linux afin d'obtenir le résultat souhaité orienté sécurité.

LAB :

- Chaque commande exécutée pour effectuer une configuration doit être notée dans le rapport final
- Le rapport final doit contenir un résumé technique et un résumé exécutif en plus des explications techniques.
- Une personne non technique doit pouvoir effectuer le même travail en lisant le rapport final. Il est donc impératif d'expliquer d'une manière très détaillée.
- Le rapport doit être rendu par mail le **18.04.2019** à **17h00** aux personnes ci-dessous :
  - bogdan@scrt.ch
  - lucie.steiner@heig-vd.ch
- Le format du fichier doit être en PDF (tout autre format ne sera pas accepté)
- Le nom du document doit avoir le format suivant :
  - date_nom1_nom2_sos.pdf

Matériel admis :

- Tout matériel ou aide est autorisé
- Toute aide extérieure ou matérielle doit être mentionnée comme source dans le rapport (créditer l'auteur original)

Remarques :

- Expliquer chaque étape entreprise pour effectuer une configuration dans le rapport.
- Ajouter des captures d'écran de vos commandes ou fichiers de configuration avec la partie modifiée.
- Justifier / expliquer les choix que vous avez faits pour effectuer les configurations.

Chargé de cours	Bogdan Nicorici
Date	Jeudi 4 avril 2019

Création d’un site internet

La société X aimerait avoir un site internet ultra sécurisé. Ce dernier sera utilisé par la suite pour des échanges financiers de haute importance. Toutes les précautions nécessaires doivent être prises afin de limiter l’impact en cas de compromission logicielle ou même physique.

Hardening système

Les contraintes de sécurité suivantes doivent être implémentées et respectées à la lettre :

- SELinux doit être désactivé
- les utilisateurs ne doivent pas voir les services/processus qui tournent sur le système
- le site doit supporter les pages dynamiques en PHP
- le service apache (httpd) doit tourner dans un conteneur docker (isoler le service apache)
    - le conteneur doit exposer le port 80 vers le port 8080 du système hôte
    - le système hôte doit rediriger le trafic du port 80 vers le port 8080 du hôte
    - le conteneur doit mapper le volume /var/www/html du système hôte sur le dossier /var/www/html utilisé par le service apache
    - le conteneur doit être supprimé dès que le service est arrêté
- le site doit afficher sur la page index.php le hostname du conteneur docker dans lequel le service apache (httpd) tourne
- le site doit être sur un file système (point de montage) de type **ext4** séparé et monté dans /var/www/**html**
- le point de pontage doit interdire l’exécution des fichiers au format binaire
- le point de montage doit interdire l’exécution des fichiers binaires avec le bit SUID
- le système de fichier doit être chiffré et monté automatiquement au démarrage avec un **mot de passe**
- le conteneur docker avec le service apache (httpd) doit démarrer automatiquement au démarrage (boot) du système hôte
- seulement l’utilisateur root doit avoir le droit de lire le fichier **/etc/sudoers** et **/etc/sudoers.d/***.
- la commande sudo doit demander le mot de passe tout le temps lorsque l’utilisateur veut lister ces droits sudo (commande : **sudo -l**) (indice : listpw)

Le système d’exploitation doit être un CentOS 7. Toutes les configurations doivent être persistantes, c’est-à-dire survivre au reboot du système.

Attribution des privilèges

Le site internet est géré par trois personnes. Les privilèges sudo pour chaque utilisateur doivent être attribués comme listé ci-dessous et de la manière la plus sécurisée possible.

NOTE : Les configurations / droits sudo doivent être effectuées sur le système hôte et non pas le conteneur docker !

- l'utilisateur **devuser** doit pouvoir **:**
  - effectuer la commande **docker pull** seulement pour le conteneur nommé « httpd »
  - démarrer (start), arrêter (stop), redémarrer (restart) le service apache dockerisé et configuré avec systemd sur le système hôte
  - activer (enable) le service dockerisé au démarrage du système hôte
  - l'utilisateur doit pouvoir lire et écrire tous les fichiers du site internet présent dans **/var/www/html** (ACL)
  - l'utilisateur doit pouvoir modifier le fichier de configurations **/etc/hosts** du système hôte

- l'utilisateur **sysuser :**
  - l'utilisateur doit pouvoir modifier tous les fichiers du site internet (ACL)
  - l'utilisateur doit faire partie du groupe **wheel**
  - l'utilisateur doit appartenir au groupe **docker**
  - l'utilisateur doit avoir tous les droits sudo (sans aucune restriction)
  - l'utilisateur doit pouvoir lister les processus sur le système (exception hidepid)

- l'utilisateur **bossuser :**
  - l'utilisateur doit seulement pouvoir lire les fichiers du site internet (ACL)
  - l'utilisateur doit pouvoir arrêter (stop), démarrer (start) le conteneur docker (service apache « httpd ») sur le système hôte
  - l'utilisateur doit pouvoir lire le fichier de configuration /etc/sudoers

Les utilisateurs ne doivent pas avoir d'autres privilèges que ceux indiqués par le client. Tout autre privilège est considéré comme une vulnérabilité dans le système.