Durcissement (hardening) d'un serveur

Le durcissement est le processus de configuration de votre serveur pour le protéger contre les attaques. Par exemple, vous pouvez **protéger par mot de passe le chargeur de démarrage GRUB** pour empêcher un attaquant de modifier le processus de démarrage. Vous pouvez également installer un outil comme ArpWatch, développé par le Lawrence Berkeley National Laboratory, pour détecter les attaques par usurpation d'adresse (ARP).

Faites attention lorsque vous durcissez votre machine car vous pouvez finir par vous verrouiller ou limiter ses capacités. Par exemple, il est courant de désactiver les compilateurs pour empêcher un attaquant de compiler des logiciels malveillants sur votre serveur. Cependant, en tant que pirate éthique, vous aurez besoin d'un compilateur pour compiler vos outils, et vous préférerez peut-être sauter cette étape de renforcement.

Le **Center for Internet Security (CIS)** tient à jour une liste de recommandations pour la sécurisation des systèmes, appelée **CIS Benchmarks**. Utilisez-les pour renforcer votre la sécurité de votre serveur et gardez-les à l'esprit lors de l'audit de la sécurité d'une entreprise. Des outils open source comme JShielder, debian-cis et nixarmor appliqueront automatiquement un grand nombre des recommandations du CIS à votre serveur. Vous pouvez installer JShielder comme suit :

```
$ git clone https://github.com/Jsitech/JShielder
```

Accédez au dossier JShielder et exécutez le script jshielder.sh (./jshielder.sh), qui vous invitera à sélectionner le système d'exploitation que vous souhaitez renforcer :

Ces outils de durcissement installent souvent des outils de détection de rootkit comme rkhunter ou chkrootkit. Ils peuvent également installer des systèmes de prévention des intrusions comme fail2ban, qui met à jour les règles de votre pare-feu pour interdire les adresses IP après plusieurs tentatives de connexion infructueuses.

De nombreux outils de renforcement automatique utilisent l'utilitaire iptables pour configurer les règles du pare-feu. Si vous souhaitez modifier vous-même les règles du pare-feu, vous pouvez

utiliser l'une des nombreuses interfaces graphiques développées pour iptables. Le meilleur est le Uncomplicated Firewall, que vous pouvez installer à l'aide de la commande suivante :

```
$ sudo apt-get install ufw
```

Après l'avoir installé, vous pouvez commencer à configurer votre pare-feu en utilisant seulement quelques commandes. Par exemple, la commande suivante définit la politique par défaut pour refuser tous les paquets entrants :

```
$ ufw default deny incoming
```

Vous pouvez ensuite commencer à ajouter des exceptions. Par exemple, nous pourrions vouloir autoriser les connexions SSH et les connexions sur le port 8080 :

```
$ ufw allow ssh
$ ufw allow 8080
```

Lorsque vous avez terminé de configurer les règles, activez le pare-feu en exécutant la commande ufw enable :

```
$ ufw enable
```

Enfin, utilisez la commande ufw status pour afficher l'état du pare-feu ainsi qu'un résumé des règles :

```
$ ufw status
```

Un autre outil utile, appelé SELinux, a été développé par la NSA et Red Hat. Il ajoute un attribut de politique supplémentaire aux fichiers du système d'exploitation. Cet attribut de politique, associé aux règles de politique SELinux, régit la manière dont ces fichiers sont accessibles et modifiés. Lorsqu'un processus tente d'accéder à un fichier, SELinux vérifie les attributs de stratégie du fichier pour déterminer si le processus est autorisé à accéder au fichier. SELinux enregistre également les accès qu'il bloque, ce qui fait de ces journaux un endroit idéal pour vérifier les intrusions suspectes.

Exécutez la commande suivante pour installer SELinux avec la stratégie par défaut :

```
$ sudo apt-get install selinux-basics selinux-policy-default auditd
```

Une fois l'installation terminée, activez SELinux et redémarrez votre système :

```
$ sudo selinux-activate
```

En plus de renforcer votre serveur, vous devez également activer le **cryptage complet du disque**.

Audit de votre serveur durci

Une fois que vous avez durci votre système, faites un audit rapide pour voir si vous avez réussi. L'outil open source Lynis vous permet d'auditer votre système par rapport aux benchmarks CIS.

Exécutez la commande suivante pour installer Lynis :

```
$ sudo apt-get install lynis
```

Ensuite, exécutez-le en utilisant sudo :

```
$ sudo lynis audit system
```

Mini-Projet 2 : Installation, configuration et sécurisation d'une application serveur

Dans ce mini-projet, vous choisirez une application serveur pour les systèmes Linux ou Windows, l'installerez, la configurerez, la sécuriserez, démontrerez sa fonctionnalité. **Ceci est un travail individuel**.

Proposition

Soumettez une proposition de projet (pas plus d'une page) qui contient les informations suivantes :

- Quelle application serveur proposez-vous d'utiliser ?
- Quel est le rôle de cette application ?
- Quelles références avez-vous qui documentent comment l'installer sur un serveur ? Fournissez les liens.
- Comment allez-vous démontrer que vous avez réussi à l'installer ?
- Quelles références avez-vous qui expliquent comment sécuriser correctement cette application ? Fournissez les liens.
- Comment allez-vous démontrer que vous avez réussi à sécuriser cette application ?

Doudou-sensei se réserve le droit de rejeter les propositions de projets dont les applications sont « trop faciles » ou qui ont été choisies par « trop » d'étudiants.

Les sujets de projet qui ne sont pas autorisés incluent, par exemple, les scripts qui auto-installent tout avec une seule commande.

Mise en œuvre

Il est maintenant temps de faire ce que vous avez proposé !

- Installez l'application serveur
- Configurez-la (selon la documentation des meilleures pratiques que vous avez trouvée)
- Sécurisez-la (selon la documentation des meilleures pratiques que vous avez trouvée)
- Démontrer qu'elle fonctionne

Suggestion : prenez des captures d'écran et des notes détaillées tout au long du processus d'installation afin de vous souvenir de ce que vous avez fait et de pouvoir le présenter à la fin.

Rapport d'installation

Au fur et à mesure de votre installation, documentez chaque étape (réussie) que vous franchissez et chaque référence que vous utilisez. Un camarade de classe devrait pouvoir suivre votre documentation et, sans consulter de références externes, arriver au même système fonctionnel que vous.

Votre rapport doit contenir :

- Une brève explication (~2 paragraphes) du système ;
- Une documentation étape par étape sur l'installation du système, y compris les commandes saisies et les captures d'écran aux étapes importantes du processus ;
- Une discussion sur la façon de configurer le système, y compris les fichiers de configuration ou autres paramètres importants ;
- Une discussion sur la façon de sécuriser le système, y compris les fichiers de configuration ou d'autres paramètres importants.

Remarque : le rapport d'installation est la partie où la plupart des points de cet exercice sont attribués. Si vous ne le documentez pas dans le rapport, je ne saurais pas que vous l'avez fait !

Exemples de sujets

- MongoDB
- NextCloud
- Jenkins
- Drupal
- Wordpress
- PostgreSQL
- Couchbase base de données NoSQL
- Jitsi : Video Conferencing Software
- Nebula : Open Source Overlay Networking
- Lychee : Self-hosted photo-management done right
- Seafile : Open Source File Sync and Share Software
- Universal Media Server
- CyberPanel
- Serveur Minecraft

- Plex Media Server
- Vaultwarden
- ProjectSend
- MySQL
- ownCloud
- Apache
- Hadoop
- Zookeeper
- Cassandra
- HDFS
- Docker
- Kubernetes
- LXC
- Etc.

Évaluation du projet

- Proposition (10 points)
- Installation (0 points) – Tous les efforts déployés ici doivent être documentés dans le rapport pour "compter"
- Rapport d'installation (90 points)

Soumission

Soumettez tous les fichiers sur le dossier Google Drive créé et partagé par les responsables de classe :

- la proposition (PDF) ;
- rapport d'installation (PDF).