Labo 01 – Linux – Confiner JtR

1. Introduction

L'objectif de ce laboratoire est de mettre en pratique certaines des techniques Linux de durcissement et confinement vues en cours.

1. Rendu attendu

Ce laboratoire doit être réalisé par groupe de 2 sauf dérogation exceptionnelle de l'équipe enseignante.

Un rapport répondant **de manière détaillée** démontrant les manipulations et répondant aux questions posées dans ce document doit être remis à la fin du travail. Les questions qui sont suivies du symbole ◉ doivent contenir une copie d'écran ou un extrait de la sortie de la console pour illustrer la réponse.

Le rapport au format **PDF** doit être rendu sur cyberlearn : https://cyberlearn.hes-so.ch/mod/assign/view.php?id=1171606

Les délais de rendu y sont indiqués. Chaque jour de retard pourra réduire la note d'un point.

NB : **respectez la numérotation des questions** dans votre rapport même s'il y a des sauts dans la numérotation.

2. Infrastructure

Il est recommandé de réaliser le laboratoire sur la VM Ubuntu préparée et utilisées pour les exercices. Un autre environnement peut être utilisé, mais sans garantie de compatibilité avec les manipulations demandées et les résultats attendus.

En cas de découverte, voire résolution de problème lié à l'environnement utilisé, merci de le partager via le forum cyberlearn : https://cyberlearn.hes-so.ch/mod/forum/view.php?id=1108732.

3. Réalisation

Un collègue (Bob) vous demande un service, il n'arrive pas à faire un exercice d'une série pour son cours de sécurité des systèmes d'exploitation. Il vous demande de l'aider en utilisant votre puissant serveur pour retrouver le mot de passe du compte 'heigvd' à partir de son hash:

```
$6$sRTLCUeE7GjlMQJm$ENy72v/H3xgc7.aLTqAaRSQ9.iQEp5uYYu4Uvy0iqt.iiycBAyxZDXrmXY25CrpDQPZbOt6Xr7l95BSx/Xd6Z.
```

Il ajoute que certaines règles (rules) semblent nécessaires pour retrouver le mot de passe et que le nom d'utilisateur a son importance.

3.1. Chroot

Vous vous méfiez de Bob, vous pouvez craindre que ce hash déclenche une porte dérobée (backdoor) dans le programme `john`, lui permettant d'accéder à votre système. Vous décidez de lancer le programme `john` (ainsi que tous les fichiers nécessaires à son exécution) dans un container `chroot`. Vous établissez le modèle d'adversaire suivant:

Le programme peut exécuter du code malveillant, il doit être isolé du système au niveau des fichiers et n'avoir accès qu'à une copie des bibliothèques et fichiers d'entrée nécessaires.

- Identifiez tous les fichiers nécessaires pour exécuter correctement le programme john, isolez le tout à l'aide de `chroot` et lancez le programme. Donnez les commandes pour la création et l'exécution du container `chroot`. (copier les ressources nécessaires, **`mount` interdit** !) **(9 pts)**
- Vous apprenez que chroot n'est pas une commande sûre et qu'il est possible de sortir du container. Démontrez un exemple de programme capable de sortir d'un `chroot`, autre que celui vu en cours. **(3 pts)**

> **Questions:**
>
> P1: Quelle est la faiblesse de `chroot` qui permet de s'en évader ? **(2 pts)**

3.2. Syscall

Vous voulez être sûr que vous ne prenez pas de risque d'évasion du `chroot`, du moins à la manière que vous venez d'identifier.

- Identifiez l'appel système (syscall) indispensable dont vous avez besoin pour sortir d'un `chroot` avec votre méthode. **(3 pts)**
- Lister tous les appels systèmes du programme `john` et vérifier que celui-ci n'utilise pas ce syscall. Donnez la commande utilisée pour avoir cette information. **(3 pts)**

> **Questions:**
>
> P2: Quelle méthode pourrait-on utiliser pour bloquer uniquement le syscall dangereux ? Expliquez la démarche complète et donner le code et les commandes destinés à empêcher ce syscall explicitement. ◉ **(10 pts)**
> (indice : https://man7.org/linux/man-pages/man2/seccomp.2.html)

3.3. Sandbox

- Empêcher le container `chroot` d'avoir accès au réseau, sans perturber le système hôte, de manière à ne pas pouvoir télécharger et exécuter de code supplémentaire. Vérifiez que votre solution bloque bien l'accès réseau en faisant un test. **(3 pts)**
  (attention au nom de la machine dans /etc/hosts)
- Autoriser le container `chroot` à avoir accès à internet, sans perturber le système hôte, et de manière à ne pas pouvoir télécharger des hashes et des scripts supplémentaires que depuis le site https://heig-vd.ch. Vérifiez que votre solution ne bloquera pas ce téléchargement alors qu'il bloque bien les autres accès réseau en faisant un test. **(6 pts)**
  (indice **:** vous pouvez utiliser l'outil **`dhclient`** du package **isc-dhcp-server** pour connecter votre container à internet et vous pouvez configurer **/etc/hosts** pour ne pas avoir à utiliser un DNS externe)

> **Questions:**
>
> P3: Malgré ces protections, pensez-vous que le programme puisse quand-même sortir de son container ? Si oui, dans quelle circonstance ? Donnez un exemple ou une référence applicable (URL). **(2 pts)**

3.4. Container

Un autre collègue (Charlie) trouve votre solution peu moderne. Il vous conseille d'utiliser l'outil docker à la place, car "il est très à la mode et utilisé par tout le monde".

- Vous décidez d'utiliser docker pour créer un container isolé sans accès réseau et capable d'exécuter le code (indice: utiliser l'image docker déjà téléchargée de https://hub.docker.com/r/phocean/john_the_ripper_jumbo). Donnez les commandes nécessaires pour la création du container, la sécurisation et l'exécution. Démontrez que votre solution bloque bien l'accès réseau en faisant un test. **(5 pts)**

Questions:

P4: Charlie revient vers vous et vous annonce qu'il propose via docker un container mieux configuré que le vôtre. Pensez-vous que cela soit une bonne idée de l'utiliser ? Pourquoi ? **(2 pts)**

P5: Vous apprenez que Bob est également un développeur très impliqué du programme `john` (que vous utilisez régulièrement). Si vous considérez Bob comme un adversaire, quelle proposition de sécurité supplémentaire pouvez-vous proposer ? **(2 pts)**

P6: Bob est également développeur du kernel Linux, notamment dans la gestion de la pile réseau. Quelle solution radicale pourriez-vous envisager afin de vous protéger contre toute attaque potentielle venant de Bob ? **(1 pt)**

3.5. John

- Quel est le mot de passe du compte heigvd correspondant au hash ? **(2 pts)**