ISE - System security

Info supplémentaires

Ce document a pour but d'apporter des informations supplémentaires pour faciliter la reproduction des exercices, notamment sur les PC de salle informatique.

La suite du document suit la même structure que le TP, pour faciliter le suivi des recommandations.

■ 1 Recovering your password

◆ 1.1 Lancer hashcat

Pour lancer hashcat depuis les salles informatiques, il est nécessaire de passer par un *conteneur* (ici, `docker`). Vous pouvez activer ce service avec les commandes suivantes :

```
dockerd-rootless-setuptool.sh
dockerd-rootless.sh || systemctl --user stop docker.service && dockerd-rootless.sh
```

Vous pouvez vérifier le bon fonctionnement de l'activation avec la commande suivante, qui devrait afficher du texte, notamment "Hello from Docker!"

`docker run hello-world`

Une fois que le service est activé, ouvrez un terminal et aller dans le dossier contenant les ressources du TP (`~/Documents/ISE/TP_system/`), et lancez l'image du conteneur à utiliser avec la commande : `docker run -it -v .:/root dizcza/docker-hashcat:intel-cpu`

Vous arriverez dans le conteneur, au sein duquel hashcat est installé et fonctionnel.

> **Sur Windows:** Si vous êtes sur Windows sur votre PC et que vous utilisez la version d'hashcat téléchargée comme indiqué dans le sujet initial, vous devrez le lancer en ligne de commande (cmd ou PowerShell) **depuis de dossier dans lequel se trouve hashcat.exe**.

◆ 1.2 Les règles hashcat

Les règles hashcat prennent la forme de fichiers texte, contenant sur chaque ligne les variations à apporter au mot de passe candidat en cours de test. Pour utiliser ces règles, il faut donc indiquer le chemin vers le fichier de règle (vous pouvez faire le TP sans soucis avec les règles dans le dossier `hashcat-6.2.6/rules/`).

◆ 1.3 Connexion SSH et identifiants sur le serveur

Pour les besoins de ce TP, je vous ai créé des comptes sur un serveur de l'Istic, mais je tiens à clarifier quelques points :

- Ce compte n'est pas votre compte sésame. Le nom d'utilisateur est similaire (voir le même pour certains/certaines), mais le **mot de passe est différent**.
- Avant de pouvoir vous connecter au serveur, vous devez retrouver votre mot de passe, dont le hashé se trouve dans le fichier `passwords_dump.txt`. Attention, ce n'est pas la même fonction de hachage que précédemment, il faudra donc changer la valeur de l'option `-m`.
- Si les approches par *bruteforce* et dictionnaire ne suffisent pas, il faudra utiliser des règles en plus (on a vu une règle particulièrement efficace...)

> Le serveur est uniquement accessible sur le sous réseau de l'ISTIC. Vous ne pourrez donc vous y connecter que depuis les salles informatique, ou le réseau eduroam.

Une fois que vous aurez retrouvé le mot de passe, vous pourrez vous connecter. Pour l'utilisateur `toto`, `sur linux`, la commande à taper sera :

```
ssh toto@ise.istic.univ-rennes1.fr
```

À la première connexion, il vous sera demandé de taper "yes" pour confirmer, puis d'entrer votre mot de passe. Vous ne verrez pas les caractères que vous tapez, c'est normal : sur linux les saisis de mot de passe se font à l'aveugle (pour éviter de divulguer la taille de votre mot de passe à quelqu'un qui regarderait par-dessus votre épaule).

> **Sur Windows:** La connexion ssh fonctionnera de manière similaire sur les version récente. Si ça ne fonctionne pas, il faudra passer par un logiciel comme PuTTY

Attention, si vous vous trompez trop de fois sur votre mot de passe, le serveur vous empêchera de vous connecter pendant une période de temps (de mémoire 30 secondes) et vous revenrra une erreur.

En cas de connexion réussie, vous aurez accès à un terminal sur le serveur, avec le message d'accueil suivant :

```
Welcome to the remote server!
```

Vous pouvez quitter cette connexion à tout moment pour revenir à votre terminal initial avec le raccourci `Ctrl+D`.

2 Secure your account credentials

- Dans cet exercice, les commandes sont à taper dans le terminal sur le serveur distant.
- Dans les questions 4.c et 4.d, si vous vous trompez dans la configuration, **vous risquez de ne plus pouvoir vous connecter au server**. Recopiez minutieusement les configurations, ou faites des copié/collé (`Ctrl+Mah+C / Ctrl+Maj+V` dans un terminal linux et clic droit dans un terminal windows).
- Pour la question 4.e (redémarrer le service ssh), vous aurez besoin de lancer la commande avec les droits d'administartion (donc en utilisant `sudo`) :
  ```
  sudo kill -HUP $(pidof sshd.pam)
  ```

En cas de soucis, contactez moi par mail : daniel.de-almeida-braga@irisa.fr