Procédure en cas de piratage d'un compte sur un serveur

En cas de problème non identifié

- Vérifier les stats Munin.
- Regarder le statut temps réel d'Apache/Nginx.
- Vérifier sur le serveur après connexion par ssh :
  - la place libre sur les disques : `df -h`
  - les commandes précédemment tapées : `history`
  - la charge du serveur : `htop`
  - le messages du noyau : `dmesg`
- Vérifier les logs ftp à la recherche d'adresses IP inconnue
- Si des fichiers ont été déposé sur le domaine par le piratage :
  - rechercher les noms de ces fichiers dans les logs du serveur web pour ce domaine
  - si une URL est trouvé extraire tous les logs de l'adresse IP ayant consulté l'URL suspecte : `cat fichier.log | grep “^adresse_ip_du_pirate” > piratage.txt`
- Lancer les outils anti-intrusions :
  - Rkhunter :
  - vérifier la version de rkhunter : `rkhunter --versioncheck`
  - mettre à jour la base de rkhunter : `rkhunter --update`
  - vérifier la présence de rootkit : `rkhunter -c`
  - si certains fichiers sont considérés comme suspects [Warning] (ex. /usr/sbin/unhide), mettre à jour après vérification de leur innocuité : `rkhunter --propupd`
  - Vérificateur de rootkit : `chkrootkit`
- Tenter de redémarrer les serveurs :
  - Apache : `/etc/init.d/httpd restart`
  - Mysql : `/etc/init.d/mysql restart`
- Vérifier les derniers fichiers modifiés sur le domaine piraté :
  - avec **find** (ex. avec les 3 derniers jours) : `find /repertoire -type f -mtime -3 -print | more`
  - avec **mc** : voir ci-dessous

Commandes utiles en cas de piratage

- Voir la taille d'un ensemble de dossier : `du -h --max-depth=1 /home/`
- Compter le nombre de fichier d'un utilisateur dans un dossier donné : `find ./ -type f -user telabotap | wc -l`
- Vérifier qu'un dossier ne contient pas de fichiers cachés : `lsattr -a`
- Rechercher les fichiers contenant une chaine de caractères particulière (plusieurs solutions) :

1) `grep "la chaine de caractère" -HnR nom_du_dossier_de_recherche`

- `grep "la chaine de caractère" -HnRo --exclude=*.svn-base nom_du_dossier_de_recherche/`

- `find nom_du_dossier_de_recherche -type f -name "*" -exec grep -Hn "la chaine de caractère" {} \;`
- Rechercher les fichiers modifiées ces 3 derniers jours : `find /repertoire -type f -mtime -3 -print | more`

Méthode pour lister tous les fichiers modifiés d'un domaine

- Se rendre dans /home/monSite/www : `cd /home/monSite/www`
- Ouvrir mc : `mc`
- Pour afficher tous les fichiers, appuyer sur les touches : `Esc` puis `?` puis `Entrée`
- Afficher les résultats en panneau, en appuyant sur : `p`
- Choisir dans le menu accessible via `F9` , l'entrée `Ordre de trie…`. Puis sélectionner avec la barre espace le tri par `date de modification`
- Examiner ensuite les fichiers modifiés récemment

En cas de piratage avéré

À faire en urgence !

- Faire sur le home concerné par le piratage : `chmod -r 000 /home/nom_du_compte_pirate`
- changer le mot de passe du compte concerné en se connectant en root puis : `passwd nom_du_compte_pirate`
- Lancer les outils anti-intrusions (rootkit) :
- Rkhunter :
  - mettre à jour la base de rkhunter : `rkhunter --update`
  - vérifier la présence de rootkit : `rkhunter -c`
- Chkrootkit : `chkrootkit`

À faire par la suite

Modifier les mots de passe :

- Générer un nouveau mot de passe sur votre ordi à l'aide de : `pwgen`
- Mysql et FTP : via webmin > OVH server > clic sur le nom de domaine > modif de mots de passe > clic sur “modifier” > redémarrez Apache
- Vérifier que le fichier `/etc/passwd` contient bien une shell sécurisé pour les utilisateurs dont on a modifié le mot de passe : `/bin/false` ou “”`/bin/MySecureShell`“”
- Changer le mot de passe de l'utilisateur : `passwd nom_utilisateur`
- htpasswd : modifier le mot de passe dans le dossier stat
- Test la connexion à Phpmyadmin, FTP…

Créer un fichier .htpasswd pour limiter l'accès au seul webmaster du site :

- créer un fichier .htpasswd à la racine du site et y mettre un login et mot de passe nouveau
- modifier le fichier .htaccess à la racine du site pour qu'il prenne en compte le fichier htpasswd