IUT Béziers
ASUR - Module ISI
TP (partie 1)

1. Etude documentaire

1.1 Recherchez et définissez les termes suivants :

- Rootkit
- 0day
- Virus
- CVE

1.2 Expliquer la notion de hash et les propriétés qu'il doit avoir.
En quoi est-ce un outil de vérification d'intégrité ?

2. Protection contre les rookits : le cas de rkhunter

2.1 Installez rkhunter 1.4.4 à partir des sources disponibles sur sourceforge.
Vous détaillerez les étapes et les commandes utilisées lors de l'installation.

2.2 Donnez les commandes nécessaires à l'analyse de votre machine.

2.3 Expliquez le principe de fonctionnement de rkhunter et la façon dont il parvient à localiser les rootkits.

2.4 Où sont stockées par défaut les empreintes de fichier réalisées par rkhunter ?
Est-ce une bonne idée en termes de sécurité ? Justifiez votre réponse.
Comment devrait-on procéder pour palier à ce défaut ?

3. Mise au point d'un rootkit élémentaire

3.1 Modifiez et recompilez la commande ls afin que l'option -42 soit rajoutée et affiche « hello IUT ». Vous détaillerez votre démarche. Installez la nouvelle commande ls sur votre système. (pensez à sauvegarder la commande originale quelquepart)

3.2 rkhunter détecte-t-il votre modification ?

3.3 Que se passe-t-il si on met à jour le système et qu'on repasse rkhunter ?

4. Tromper rkhunter

4.1 Modifiez la commande de hash (sha256) utilisée par rkhunter afin que celle-ci affiche toujours le même résultat, quelquesoit le fichier « /bin/ls » présent sur le système. Montrez que, avec cette méthode, rkhunter peut être trompé et ne détecter aucune modification.

4.2 Expliquez comment modifier directement rkhunter afin qu'il ne remonte aucune alerte.

4.2 Ecrivez une procédure détaillée d'analyse d'une machine avec rkhunter.