SE - BLOC2 - UE28 - Monitoring

Laboratoire 1

Ludewig François

1 Objectifs

L'objectif de ce laboratoire est la découverte des messages de log générés par le système d'exploitation **Kali - Linux**.

A la fin de laboratoire l'étudiant sera capable de :

1. de localiser les messages de log ;
2. d'utiliser les outils pour la lecture des messages de log ;
3. d'identifier les composants d'un message de log ;
4. de classifier [taxinomie] les messages de log ;
5. d'identifier les priorités des messages de log.

1.1 Consignes

Tous les membres du groupes doivent réaliser l'ensemble de ce laboratoire de façon individuel. Cela n'exclus pas de trouver de l'aide et du support au sein de son groupe.

Deux séances de 2 heures seront consacrées à ce laboratoire.

2 Mise en place

Pour réaliser ce laboratoire, vous devez

* télécharger une machine virtuelle Kali-Linux ;
* démarrer la machine virtuelle dans VMWare Workstation Pro ;
* créer un compte avec vos crédential HELMo ;
* vous octroyer les droits sudo.

3 Démarche à suivre

Voici la liste des étapes à suivre pour réaliser le laboratoire.

3.1 Localisation et outils

Rendez-vous dans le dossier **/var/log/**. Analyser les fichiers ainsi que leur organisation en sous répertoires. Pour ce faire vous pouvez vous aider des outils suivants :

1. ls
2. tree
3. more
4. awk
5. grep
6. ...

Prenez le temps de lire le manuel des commandes linux pour bien les exploiter. Cela peut vous faire gagner beaucoup de temps.

3.2 Lecture

Identifier les différentes informations présentes dans les messages de chaque fichier. Attention leur localisation est une information en elle-même.

Déterminer la(les) taxinomie(s), aidez-vous des exemples vus au cours théorique. Etablissez l'échelle de priorité des messages de log.

Quels sont les messages de logs en relation avec la sécurité du système d'exploitation ?

3.3 Rapport

Réaliser un rapport qui présentera votre analyse illustrée d'exemples.

Ce dernier doit décrire

1. **la(les) taxinomie(s) ;**
2. **l'échelle de priorité que vous avez identifiés ;**
3. **les informations détaillées relatives à la sécurité que vous aurez désigner ;**

Une section du rapport doit être consacrée à votre démarche et aux difficultés rencontrées.

Vous êtes libres du choix de l'outil pour la rédaction du rapport (word, latex, ...). Néanmois, ce dernier doit faire mention du cours, du numéro du groupe, du nom et prénom de tous les étudiants du groupe.