SE - BLOC2 - UE28 - Monitoring

Laboratoire 2

Ludewig François

1 Objectifs

L'objectif de ce laboratoire est la découverte des messages de log générés par le système d'exploitation **Windows Server / Windows 10**.

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

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

1.1 Consignes

Tous les membres du groupes doivent réaliser l'ensemble de ce laboratoire individuellement. Cela n'exclut 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 Windows Server ;
* démarrer la machine virtuelle dans VMWare Workstation Pro ;
* créer un compte avec vos crédential HELMo ;
* vous octroyer les droits administrateur.

3 Démarche à suivre

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

3.1 Localisation et outils

Analyser les fichiers ainsi que leur organisation en sous répertoires. Pour ce faire vous pouvez vous aider des outils suivants : **Event Log**. 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. Établir 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 Configurer et exploiter

L'outil **Event Log** ne se limite pas à la présentation élégante des logs générés dans le système d'exploitation de Windows.

Il permet de réaliser des tâches comme le filtre et le forward. Nous allons dans ce laboratoire nous intéresser à la partie filtre.

Deux technique permettent de mettre en place des filtres de message de log de Windows. Il est possible d'effectuer un filtre sur un journal que vous consulter. Une vue personnalisée peut être définie pour isoler et visualiser les messages de logs d'intérêt.
Réaliser les filtres suivants :

- Créer une vue personnalisée qui vous permet de trouver les messages de logs relatifs aux connexions des utilisateurs et aux démarrages / arrêt de la machineS.

- Dans les journaux windows,réaliser un filtre pour ne voire que les messages de niveau critique et erreur. Réaliser une analyse, recherche afin de comprendre les erreurs identifier grâce aux filtres.

3.4 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 identifiée ;**
3. **les informations détaillées relatives à la sécurité que vous aurez désignées ;**
4. **une comparaison avec l'analyse réalisée pour Kali-Linux lors du premier laboratoire.**
5. **une description de votre enquête afin de comprendre les erreurs identifier sous Windows (5 erreurs différentes)**

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.