SE - BLOC2 - UE28 - Monitoring

Laboratoire 3

Ludewig François

1 Objectifs

L'objectif de ce laboratoire est l'installation et la mise en œuvre d'un écosystème de logs, via l'utilisation d'une implémentation SysLog pour centraliser les messages de log générés par le système d'exploitation **Kali-Linux**, **Windows** et **Android**.

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

1. Installer et configurer un daemon Syslog comme LogHost (LogCollector) sous Linux et Windows.
2. Installer et configurer un daemon Syslog comme agent de log (transfert des messages de log aux collecteurs) sous Linux et Windows.
3. Installer et configurer un daemon Syslog comme agent de log (transfert des messages de log aux collecteurs) sous Android.

1.1 Consignes

Tous les laboratoires sont réalisés en groupe. Pensez à bien répartir votre travail et à maintenir une communication. Il n'y a qu'un seul rapport à faire par groupe.

Quatre séances de 2 heures seront consacrées à ce laboratoire.

2 Démarche à suivre

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

2.1 RSyslog sous Kali-Linux

Dans un premier temps vous allez installer Syslog sous votre machine Kali-Linux. Ce dernier permet de centraliser et de normaliser dans une certaine mesure les messages de log.

2.1.1 Outils

Installer une implémentation de SysLog sur Kali-Linux.

Lire attentivement le manuel de l'implémentation que vous avez sélectionnée.

Analyser pour comprendre et maitriser le fonctionnement des "daemon" sous Linux.

2.1.2 Configuration

Choisir et établir une configuration de votre Daemon, sur base des informations et principes présentés au cours théorique.

Tester plusieurs configurations : fichiers non indexés ou fichiers indexés.

Justifier les configurations mises en œuvre.

2.1.3 Analyse

Que sont devenus les messages de log identifiés lors du premier laboratoire ?

Mettre en correspondance les messages de logs de SysLog et ceux du système d'exploitation.

Comment la configuration Syslog influence-t-elle cette correspondance ?

2.2 Centralisation des logs - Kali-Linux

Il est possible de configurer les daemons SysLog afin de mettre en place un éco-système de log. De fait vous allez mettre en place un LogHost ou Collecteur de logs et des agents "forwarder" émetteurs de messages de log.

2.2.1 Outils

Lire attentivement la documentation de RSysLog.

Afin que vos machines Linux virtuelles ou non communiquent, vous devez activer le VPN. Dans le fichier helmocg.vpn (téléchargé depuis HELMo Learn pour OS X), ajouter à la fin :

1. remote-cert-tls server
2. script-security 2
3. up /etc/openvpn/update-resolv-conf
4. down /etc/openvpn/update-resolv-conf

Si openvpn n'est pas installé, lancer la commande : "sudo apt-get install openvpn". Lancer openVPN dans un terminal via la commande : "sudo /usr/sbin/openvpn -config helmocg.ovpn -auth-user-pass -auth-retry interact". Encoder vos crédential de HELMo et le vpn démarre.

Dans un autre terminal, vous pouvez lancer la commande "ip a" pour voir la configuration réseau de la machine et vérifier si le vpn est bien en route.

2.2.2 Configuration

Chaque membre du groupe doit configurer :

1. sa machine virtuelle Kali-Linux en mode LogHost afin de collecter les logs des autres membres du groupe.
2. sa machine virtuelle Kali-Linux en mode forward afin de transmettre ses logs aux LogHosts des autres membres du groupe.

2.2.3 Analyse

Tous les messages de log sont-ils présents sur le collecteur de log ? Comment la configuration Syslog influence-t-elle cette sélection ?

2.3 RSyslog sous Windows et Centralisation cross-plateforme

Au-delà du système propriétaire de log de Windows : Event Log, il est possible de mettre en place une centralisation des messages de logs cross-plateforme. Une implémentation de SysLog pour Windows existe. Cette dernière permet de convertir et normaliser les messages de Windows avant de les transmettre à un loghost ou un collecteur de logs.

2.3.1 Outils

Installer une implémentation de SysLog sur Windows Server 2016 et/ou sur Windows 10.

Lire attentivement le manuel de l'implémentation que vous avez sélectionnée.

2.3.2 Configuration

Choisir et établir une configuration de votre application Syslog, sur base des informations et principes présentés au cours théorique. Configurer vos Windows pour qu'il transmette les messages de log aux loghost de votre groupe.

Justifier les configurations mises en œuvre.

2.3.3 Analyse

Que sont devenus les messages de log identifiés lors du précédent laboratoire ?

Mettre en correspondance les messages de logs de SysLog et ceux du système d'exploitation.

Comment la configuration Syslog influence-t-elle cette correspondance ?

2.4 Android comme source de logs

Comme vous le savez, un grand nombre de système informatique sont susceptibles de produire des messages de log. Parmi ceux-ci, votre smart-phone ne déroge pas à la règle. Vous allez maintenant apprendre à activer les messages de logs sous Android, visualiser et analyser les messages d'alerte, erreur ou critique que vous allez identifier. Finalement, vous allez centraliser les messages de logs générés par Android sur tous les loghost de votre groupe.

2.4.1 Outils

Vous allez devoir installer des applications qui vous aideront à réaliser cette tâche :

1. SysLog

2. Logcat to UDP

Il vous faudra configurer votre smartphone pour qu'il transmette vos messages de log via l'application "Logcat o UDP". Voici quelques liens utiles :

1. How to forward Android syslog
2. How to Access Developer Options and Enable USB Debugging on Android
3. How to use ADB to grant permissions
4. How To Enable & Disable Developer Options On Your Android Device

2.4.2 Configuration

Choisir et établir une configuration de votre application Syslog, sur base des informations et principes présentés au cours théorique. Configurer vos Android pour qu'il transmette les messages de log aux loghost de votre groupe.

Justifier les configurations mises en œuvre.

2.4.3 Analyse

Examiner les messages de log en provenance de votre Android, identifiez la taxonomie et l'échelle de priorité des messages. Réaliser un recherche afin de comprendre les messages d'erreur de votre Android.

3 Rapport

Continuer votre rapport qui présentera votre analyse illustrée d'exemples.

Ce dernier doit contenir les points suivants :

1. **une présentation des configurations de SysLog ;**
2. **une discussion autour de la mise en oeuvre des principes de log.**

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

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