SE - BLOC2 - UE28 - Monitoring

Laboratoire 5

Ludewig François

1 Objectifs

L'objectif de ce laboratoire est la mise place d'un programme de récupération de données de monitoring à l'aide du protocole SNMP.

A la fin du laboratoire l'étudiant sera capable :

1. de lire et faire des recherches dans une MIB
2. de faire configurer un server SNMP sur une machine agent
3. de programmer des requêtes SNMP pour récupérer des valeurs
4. d'analyser et de présenter les données récupérées de façon adaptées à leur nature.

2 Démarche

Voici les étapes principales à suivre pour faire ce laboratoire

2.1 Configurer SNMP

Vous devez mettre en place une architecture SNMP tel que décrite au cours théorique en parallèle de votre écosystème de messages de log.

Pour ce faire, vous devez installer et configurer un serveur SNMP sur les agents. Ce serveur SNMP répondra aux requêtes du manager.

Le manager sera "simuler" par l'utilisation des commandes consoles vue au cours théorique. Vous pouvez si vous le souhaitez utiliser un autre logiciel sous Linux ou même sous Windows.

2.2 Données de configuration

L'objectif est récolter un maximum d'informations, de configuration, des agents utiles à la surveillance et à la sécurité du système informatique.

Allez à la découverte de la MIB à l'aide d'outil proposé. N'hésitez pas à faire des recherches par vous même en parallèle. Vous devez au minimum être capable de récupérer les informations relatives :

1. au système (Nom, Type, ...)
2. à la configuration CPU
3. à la configuration des mémoires (disque, RAM, ...)
4. à la configuration des interfaces
5. ...

Vous devez mettre présenter de façon adéquate les données récoltées au travers de graphiques, tableaux, ... Discutez vos observations et tirez les bonnes conclusions.

2.3 Données de surveillance

L'objectif est récolter un maximum d'informations, de surveillance, des agents utiles à la surveillance et à la sécurité du système informatique.

Allez à la découverte de la MIB à l'aide d'outil proposé. N'hésitez pas à faire des recherches par vous même en parallèle.

Pour cette partie, un programme de stress tournera sous une machine KALI de votre groupe ou commune à tous afin de simuler une activité que vous allez devoir détecter.

Il s'agit ici de surveiller en temps réel l'évolution des métriques de surveillance le machine. Vous devez donc développer un outils (programme Python, script, ...) pour récolter les données toutes les secondes pendants 4 minutes.

Vous devez être capable de récupérer les informations relatives :

1. à l'usage du CPU
2. à l'usage de RAM
3. aux flux entrant et sortant des interfaces
4. à l'usage des disques

Vous devez mettre présenter de façon adéquate les données récoltées au travers de graphiques, tableaux, ... Discutez vos observations et tirez les bonnes conclusions.

3 Outils

Une liste d'outils utiles pour la réalisation du laboratoire est proposée sur l'espace de cours. Vous pouvez réaliser certaines tâches à l'aide d'autres outils comme : programme en Python, scriptes en Shell, Bash ou Perl, ...

3.1 Rapport

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

Ce dernier doit contenir pour chaque scénario les points suivants :

1. **Une description des données récoltées**
2. **L'analyse des valeurs reçues**
3. **La présentation des valeurs de façon cohérente au regard de leur type.**

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, ...). Néanmois, ce dernier doit faire mention du cours, du numéro du groupe, du nom et prénom de tous les étudiants du groupe.