SE - BLOC2 - UE28 - Monitoring

Laboratoire 4

Ludewig François

1 Objectifs

L'objectif de ce laboratoire est de réaliser des scénarios dont vous devrez identifier les traces et engendrer quand cela est possible une action "simple".

A la fin du laboratoire l'étudiant sera capable :

1. d'analyser les données pour identifier les traces d'un scénario
2. de mettre en place un système de détection du dit scénario
3. de provoquer une action automatique lors de la détection.

2 Démarche

Voici les étapes principales à suivre pour réaliser les différents scénarios :

1. produire le scénario
2. identifier les traces générées par ce dernier
3. établir, configurer ou construire un outil de détection du scénario
4. choisir et programmer une action à entreprendre en cas de détection
5. mettre en place cet outil et le tester.

Différentes actions sont possibles (liste non exhaustive) :

1. générer un log : soyez attentifs aux informations de votre message de log : taxonomie, priorité, ...
2. écrire un message dans la console d'un ou plusieurs utilisateurs
3. envoyer un email
4. activer un script

Certains traitements peuvent être réalisés sur les machines agents (surveillées) mais les actions seront réalisées uniquement par le manager (loghost, logCollector).

Vous devez implémenter chaque action au moins une fois, pour un des scénario. De plus, pour chaque scénario, vous avez l'obligation de générer un message log adéquat.

3 Scénarios

Vous devez réaliser l'ensemble des scénarios proposés ci-dessous.

3.1 Fonctionnalité

Il est important dans un système informatique d'une entreprise de détecter si les appareils sont bel et bien en fonction. Vous devez être capable de détecter le redémarrage d'un pc. Il existe plusieurs méthodes pour atteindre cet objectif. Choisissez celle qui vous semble la plus adéquate.

3.2 Tentatives de connexion

Dans le cadre d'une attaque, il est possible que l'attaquant effectue une série de tentatives de connexion avant de réussir ou pas. De même, un utilisateur officiel d'une machine peut effectuer des erreurs en se connectant sur une machine.

Vous devez être capable de détecter une série d'échecs de connexion suivis par une réussite. Identifier s'il s'agit d'une attaque ou non, agir en conséquence.

Lors d'un échec d'un utilisateur valide. Il se peut que ce dernier, par erreur de manipulation, ait écrit son mot de passe avec son identifiant. Son mot de passe est donc logiquement lisible quelque part. Détecter un tel cas et décider des actions à mener.

3.3 DoS détection

Une attaque de type DoS consiste à bombarder de connexions ou de requêtes un serveur ou un système informatique. Dans sa version non distribuée, l'attaque est émise depuis un même ordinateur.

Un moyen de se protéger contre une attaque basique de type DoS est de détecter la mise en place de plusieurs connexions sur un de vos pc/serveur depuis l'ordinateur émetteur de l'attaque.

Plus précisément : détecter deux connexions utilisant le même protocole en provenance d'une seule et même machine.

Extension : détecter la réception de requêtes en provenance d'un même ordinateur attaquant sur votre serveur. L'outil tcpdump peut être utile dans la réalisation de cette tâche.

3.4 Interdire l'administration à distance

Un changement de configuration est un événement à ne pas négliger dans le cadre du monitoring d'un système informatique.

Plus particulièrement, certaines machines sont sensibles pour le réseau, pour les services ou les données. Une approche possible est de simplement interdire la configuration à distance sur de telle machine.

Vous devez être capable de détecter que quelqu'un réalise des actions en tant que "super utilisateur" à distance.

3.5 Interdire la connexion en cascade

Une connexion en cascade n'est un schéma habituel dans un système informatique d'une entreprise. Cela relève d'un comportement douteux qui doit attirer l'attention de l'équipe de monitoring.

Un utilisateur lambda ne doit pas se connecter depuis son pc à un pc3 via un pc2 intermédiaire.

Vous devez être capable de détecter un tel comportement sur votre réseau.

3.6 Faille Sudo

Récemment une faille sudo a été dévoilée et aussitôt résolue par un patch. Néanmoins, il n'en sera pas ainsi pour chaque faille. Dans l'attente d'une mise à jour qui restaurera la sécurité de votre système informatique, vous devez mettre en place des outils de détection. Ces derniers vous permettront de réagir au plus vite en cas d'utilisation d'une faille connue mais non résolue.

Renseignez-vous sur cette faille : ici. Adaptez votre système afin qu'il présente cette faille.

Détectez les traces de l'utilisation de cette faille pour ensuite établir un système de détection et agir en conséquence.

3.7 Promiscuous

Le mode promiscuous d'une interface réseau lui permet de recevoir tous les paquets du réseau, même ceux qui ne lui sont pas destinés (MAC adresse différente). Ce mode peut-être utilisé par des outils de monitoring. Néanmoins, en dehors de ces outils, son utilisations sera

susceptible d'être liée à sniffer qui analyse le trafic de votre réseau.

Vous devez donc être capable de détecter le passage d'une interface d'une machine du réseau dans ce mode particulier.

3.8 Extension A : Courriel

Tout comme pour les connexions vers des domaines inconnus sont à surveiller voir même à interdire, il est primordial de surveiller les destinations des emails sortant de l'entreprise ainsi que la nature des pièces jointes.

Pour ce scénario, vous devez configurer un client mail avec votre adresse HELMo. Effectuer des échanges entre vos adresses HELMo et externes. Détecter l'envoi de messages hors de l'institut HELMo et si possible la présence de pièces jointes.

3.9 Extension B : Scanneur de port

Le "scan" des ports de machines de votre réseau est souvent une action menée en amont de la véritable attaque. Il est donc important de détecter ce type de menace.
Vous devez être capable de détecter une telle action sur les machines de votre réseau. Selon la qualité de l'attaque, vous aurez besoin des messages de logs, d'un IDS ou d'un firewall.

3.10 Extension C : Votre scénario

Si et seulement si vous avez fini l'ensemble des scénarios proposés, vous pouvez alors établir votre propre scénario : une attaque sur les services de log, une attaque plus perfectionnée d'un des scénarios proposés, ou autre. Le faire valider par votre enseignant.

4 Outils

Une liste d'outils utiles pour la réalisation des scénarios est proposée sur l'espace de cours. L'application SEC, présentée au cours théorique, permet de mettre en œuvre les règles utiles à l'analyse des messages de log. Vous pouvez réaliser certaines tâches à l'aide d'autres outils comme : programme en Python, scriptes en Shell, Bash ou Perl, ...

4.1 Rapport

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

Ce dernier doit contenir pour chaque scénario les points suivants :

1. **Une description de la mise en œuvre du scénario**
2. **L'explication et la justification de la méthode de détection employée**

3. **La description du log émis lors de la détection (exemple) et de l'action complémentaire.**

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.

Les scripts, les règles SEC ou autres programmes doivent être transmis comme pièces jointes aux rapports.