Comment est-ce que je peux identifier et adresser une situation de boucle de messagerie sur l'ESA?

Contenu

Introduction

Ce document explique comment repérer une boucle de messagerie sur le dispositif de sécurité du courrier électronique (ESA).

Informations générales

Des boucles de messagerie peuvent être indiquées par les messages dont le même identifiant a été injecté plus de trois fois. Les boucles de messagerie peuvent présenter des symptômes liés à des problèmes de surutilisation du CPU, de transmission lente et de rendement global. Normalement les identifiants de message injectés plus d'une fois indiquent un cas de bouclage. Néanmoins, ils sont parfois injectés plus d'une fois en raison de problèmes, ou à cause d'un polluposteur mal réglé qui continue d'injecter le même pourriel avec le même identifiant de message.

De manière plus courante, une boucle de messagerie est provoquée par des problèmes liés aux infrastructures de messagerie qui envoient le même message ou une série de messages qui se précipitent dans tous les recoins de votre réseau, de serveurs de messagerie à d'autres serveurs de messagerie dans une course sans fin. Tandis que ces boucles de messages peuvent ainsi s'entretenir d'elles-mêmes pendant très longtemps, elles grugent la bande passante de votre réseau et accroissent les coûts effectifs du traitement ESA.

Solution

Si vous croyez qu'il s'agit de la cause du problème, repérer une boucle de messagerie est habituellement assez facile, mais vous devrez la rechercher.
Connectez-vous dans l'interface de ligne de commande (CLI) du système et exécutez une de ces commandes, ou les deux, selon ce qui est plus efficace pour vous :

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

Lorsqu'il est particulièrement question de la recherche sur l'identifiant de message, des exemples récurrents du même identifiant vous indiquent que vous êtes en présence d'une boucle de messagerie. Néanmoins ce n'est pas toujours suffisant, car parfois, un des serveurs de messagerie renvoyant le même message modifiera ou supprimera l'en-tête de l'identifiant du message. Ainsi, si vous n'obtenez aucun résultat identifiable lors de la vérification de l'identifiant du message, passez à la vérification de l'objet.

En supposant que vous avez réussi à trouver le message de bouclage grâce à l'identifiant de message, vous voudrez également découvrir d'autres informations sur le message et sa connexion parente (ICID). Lorsque l'identifiant du message et un MID sont sur la même ligne de journal, vous pouvez exécuter :

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

Vu le résultat ici obtenu, vous pouvez trouver l'ICID et leDCID appropriés et effectuer :

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

Vous devriez maintenant avoir la transaction complète de la connexion au message, et être en mesure de voir d'où il provient et où il a été envoyé (si elle est déjà complétée). Une fois que vous avez trouvé le message de bouclage, l'étape suivante est de jeter un coup d'œil de sorte que vous puissiez résoudre le problème. Si l'on ne s'attaque pas à la cause de la boucle, il est probable que ce message, ainsi que d'autres, continuent de faire une boucle ou que le problème se reproduise bientôt.

Créez un filtre de message semblable à celui-ci :

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

Effectuez maintenant cette modification et exécutez cette commande pour vérifier le message :

```
tail looper
```

Grâce aux renseignements que vous pouvez trouver au sujet du système distant en regardant les journaux de messagerie, ainsi que d'autres informations que vous pouvez obtenir en regardant le message lui-même, vous devriez être en mesure de déterminer où se trouve votre problème.

Comment empêcher des boucles de messagerie de se produire?

Dans les environnements complexes, cette tâche peut être ardue, car il est essentiel de savoir comment les courriels se diffusent dans votre environnement pour voir comment une modification de réseau, sur l'ESA ou sur un autre périphérique, influera sur le trafic. Une cause fréquente de l'emballement des boucles de messagerie est la suppression de l'en-tête Reçu. L'ESA détectera et arrêtera automatiquement une boucle de messagerie s'il constate 100 en-têtes Reçu dans un message. Toutefois, l'ESA tient compte de la suppression de cet en-tête, menant ainsi souvent à une mauvaise boucle de messagerie. À moins d'avoir une *très* bonne raison de le faire, vous ne devez pas désactiver l'en-tête Reçu, ou faire en sorte qu'il soit supprimé.

Vous trouverez ci-dessous un exemple de filtre qui peut vous aider à empêcher ou à régler un problème de boucle de messagerie :

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```