Localisez les informations d'alerte DHAP sur l'ESA

Contenu

Introduction

Ce document décrit comment localiser les informations en vue de des alertes de la prévention d'attaque de récolte de répertoire (DHAP) sur votre appliance de sécurité du courrier électronique de Cisco (ESA).

Localisez les occurrences DHAP de l'ESA

Les entrées qui décrivent l'événement DHAP résident dans les logs de messagerie. Voici une entrée de journal de messagerie d'exemple quand DHAP se produit :

```
Tue Oct 18 00:25:35 2005 Warning: LDAP: Dropping connection due to potential Directory
Harvest Attack from host=(192.168.10.1', None), dhap_limit=4, sender_group=SUSPECTLIST
```

> Remarque: Par défaut, le netmask de **/24** est recherché dans la recherche.

Écrivez cette requête dans le CLI afin de visualiser les logs de messagerie :

```
myesa.local> grep "dhap_limit=" mail_logs
```

Les compteurs DHAP incluent des rejets réceptifs de requête de rejets de Tableau d'Access (RAT) et d'acceptation de Protocole LDAP (Lightweight Directory Access Protocol). Les configurations DHAP sont configurées dans la stratégie de flux de courrier.

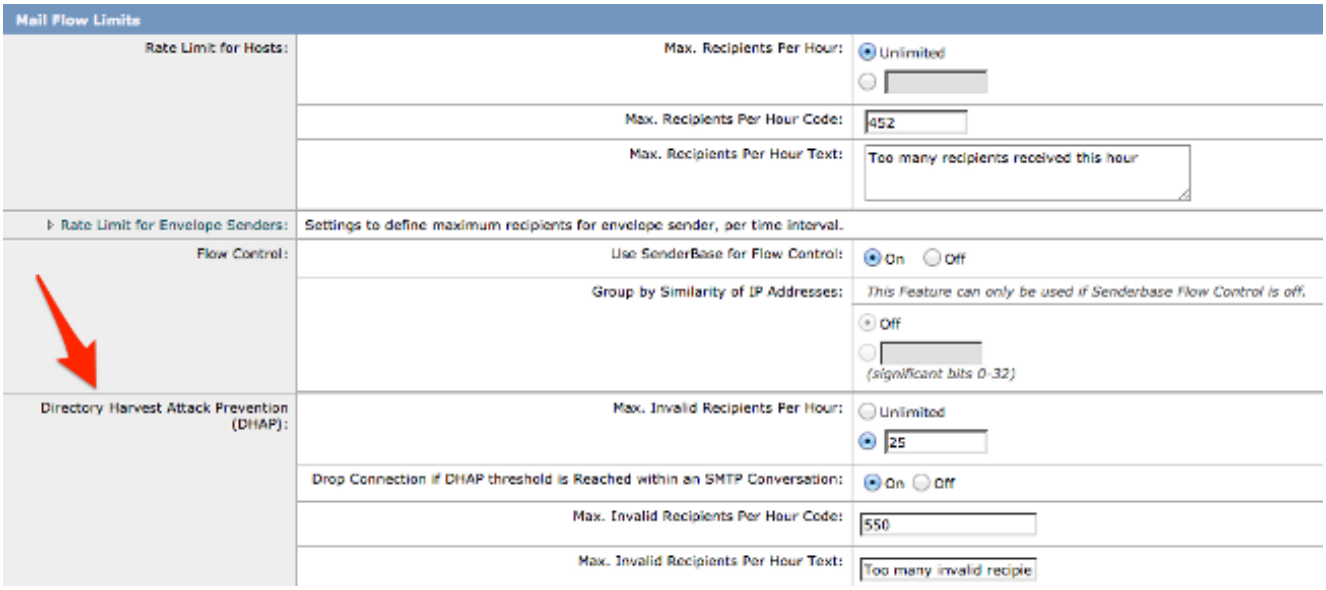
Configuration de vue ou de mise à jour DHAP du GUI

Terminez-vous ces étapes afin de visualiser ou éditer vos paramètres de configuration DHAP du GUI :

1. Naviguez **pour envoyer par mail des stratégies > des stratégies de flux de courrier**.

2. Cliquez sur le nom de stratégie afin de faire édite, ou clique sur des **paramètres de stratégie par défaut** afin de visualiser la configuration du courant DHAP.

3. Apportez des modifications à la section de la **prévention d'attaque de récolte de répertoire (DHAP)** comme nécessaire :



4. Cliquez sur Submit, et puis cliquez sur la **validation** afin de sauvegarder vos modifications.

Configuration de vue ou de mise à jour DHAP du CLI

Afin de visualiser ou éditer vos paramètres de configuration DHAP du CLI, écrivez le **listenerconfig > éditent [*nombre d'auditeur*] > des hostaccess >** commande de **par défaut** :

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 5 policies defined.
There are currently 8 sender groups.
```

```
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for
megabytes, or no letter for bytes.
[10M]>

Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.
[550]>

Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
```

```
5. Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing? [N]>

Would you like to enable DKIM verification? [N]>

Would you like to change SPF/SIDF settings? [N]>

Would you like to enable DMARC verification? [N]>

Would you like to enable envelope sender verification? [N]>

Would you like to enable use of the domain exception table? [N]>

Do you wish to accept untagged bounces? [N]>
```

Si vous choisissez de faire des mises à jour, assurez-vous que vous revenez à la demande principale CLI et **commettez** toutes les modifications.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco – Guides d'utilisateur
- Support et documentation techniques - Cisco Systems