Procédures principales de capture de paquet d'infrastructure

Contenu

Introduction

Ce document décrit l'utilisation de la commande CLI de **tcpdump** afin de capturer les paquets désirés d'un serveur de l'infrastructure de perfection de Cisco (pi).

Utilisez la commande de tcpdump

Cette section fournit les exemples qui montrent la manière dans laquelle la commande de **tcpdump** est utilisée.

```
nms-pi/admin# tech dumptcp ?
<0-3> Gigabit Ethernet interface number
```

La sortie de la **commande d'interface d'exposition** fournit des informations précises au sujet du nom et du nombre d'interface qui est actuellement en service.

```
nms-pi/admin# tech dumptcp 0 ?
count Specify a max package count, default is continuous (no limit)
<cr> Carriage return.
```

> **Note**: Vous pouvez mettre en boîte indiquez le compte spécifique de module dans la commande précédente. Si vous n'indiquez pas un compte spécifique de module, une capture continue est exécutée sans la limite.

```
nms-pi/admin# tech dumptcp 0 | ?
Output modifier commands:
begin Begin with line that matches
count Count the number of lines in the output
end End with line that matches
exclude Exclude lines that match
include Include lines that match
last Display last few lines of the output
```

```
nms-pi/admin# tech dumptcp 0 > test-capture.pcap
```

Note: Il est le plus facile de sauvegarder le fichier, et puis le passe en revue. Dans cet exemple, le serveur enregistre le fichier dans la racine de la structure de répertoire. Afin de visualiser les fichiers, sélectionnez la commande de **dir**.

Copiez les fichiers capturés sur un emplacement extérieur

Voici deux exemples qui montrent la manière dans laquelle a capturé des fichiers sont copiés sur un emplacement qui est en dehors de du serveur :

- Dans cet exemple, le fichier de capture est copié sur un ftp server avec une adresse IP de **1.2.3.4** :

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- Dans cet exemple, le fichier de capture est copié sur un serveur TFTP avec une adresse IP **5.6.7.8** :

  ```
  copy disk:/test-capture.pcap tftp://5.6.7.8/
  ```

Paquets de capture en tant qu'utilisateur de base

Si vous désirez des captures plus granulaires, connectez-vous dans le CLI pendant qu'un *utilisateur de base* après que vous ayez ouvert une session en tant qu'utilisateur d'*admin*.

```
test$ ssh admin@12.13.14.15
Password:
nms-pi/admin#
nms-pi/admin# root
Enter root password :
Starting root bash shell ...
ade # su -
[root@nms-pi~]#
```

Captures d'utilisateur de base d'exemple

Voici trois exemples des captures qui sont prises par un utilisateur de base :

- Dans cet exemple, tous les paquets qui sont destinés au port **162** sur le serveur pi sont capturés :

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- Dans cet exemple, tous les paquets qui sont destinés au port **9991** sont capturés et écrits à un fichier appelé le **test.pcap dans le répertoire de** /localdisk/ftp/ :

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- Dans cet exemple, tous les paquets avec une adresse IP source de **1.1.1.1** sont capturés :

```
[root@nms-pi~]# tcpdump -n src host 1.1.1.1
```