Procédures de capture de paquets Prime Infrastructure

Contenu

Introduction

Ce document décrit l'utilisation de la commande CLI **tcpdump** afin de capturer les paquets souhaités à partir d'un serveur Cisco Prime Infrastructure (PI).

Utiliser la commande tcpdump

Cette section fournit des exemples illustrant la façon dont la commande **tcpdump** est utilisée.

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

Le résultat de la commande **show interface** fournit des informations précises sur le nom et le numéro de l'interface actuellement utilisés.

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

> **Note**: Vous pouvez indiquer le nombre de paquets spécifique dans la commande précédente. Si vous n'indiquez pas de nombre de paquets spécifique, une capture continue est exécutée sans 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 plus facile d'enregistrer le fichier, puis de le consulter. Dans cet exemple, le serveur enregistre le fichier à la racine de la structure de répertoires. Pour afficher les fichiers, entrez la commande **dir**.

Copier les fichiers capturés vers un emplacement externe

Voici deux exemples illustrant la manière dont les fichiers capturés sont copiés vers un emplacement situé en dehors du serveur :

- Dans cet exemple, le fichier de capture est copié sur un serveur FTP avec l'adresse IP **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/
  ```

Capture des paquets en tant qu'utilisateur racine

Si vous souhaitez des captures plus granulaires, connectez-vous à l'interface de ligne de commande en tant qu'utilisateur *racine* après vous être connecté en tant qu'utilisateur *administrateur*.

```
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~]#
```

Exemple de capture d'utilisateur racine

Voici trois exemples de captures prises par un utilisateur root :

- Dans cet exemple, tous les paquets 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 destinés au port **991** sont capturés et écrits dans un fichier appelé **test.pcap** dans le **/localdisk/ftp/** répertoire :

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

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