Procedimientos de captura de paquetes de infraestructura Prime

Contenido

Introducción

Este documento describe el uso del comando CLI **tcpdump** para capturar los paquetes deseados de un servidor de Cisco Prime Infrastructure (PI).

Utilice el comando tcpdump

Esta sección proporciona ejemplos que ilustran la forma en que se utiliza el comando **tcpdump**.

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

La salida del comando **show interface** proporciona información precisa sobre el nombre de la interfaz y el número que se está utilizando actualmente.

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

> **Nota:** Puede indicar el conteo de paquetes específico en el comando anterior. Si no indica un conteo de paquetes específico, se ejecuta una captura continua sin límite.

```
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
```

Nota: Es más fácil guardar el archivo y después revisarlo. En este ejemplo, el servidor guarda el archivo en la raíz de la estructura de directorios. Para ver los archivos, ingrese el comando **dir**.

Copiar los archivos capturados en una ubicación externa

Estos son dos ejemplos que ilustran la forma en que se copian los archivos capturados en una ubicación que se encuentra fuera del servidor:

- En este ejemplo, el archivo de captura se copia en un servidor FTP con una dirección IP de **1.2.3.4**:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- En este ejemplo, el archivo de captura se copia a un servidor TFTP con una dirección IP **5.6.7.8**:

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

Capture paquetes como usuario raíz

Si desea más capturas granulares, inicie sesión en la CLI como usuario *raíz* después de haber iniciado sesión como *usuario administrador*.

```
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~]#
```

Ejemplo de capturas de usuario raíz

A continuación se muestran tres ejemplos de capturas realizadas por un usuario raíz:

- En este ejemplo, se capturan todos los paquetes destinados al puerto **162** en el servidor PI:

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- En este ejemplo, todos los paquetes destinados al puerto **991** se capturan y escriben en un archivo llamado **test.pcap** en el directorio **/localdisk/ftp/**:

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- En este ejemplo, se capturan todos los paquetes con una dirección IP de origen de **1.1.1.1**:

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