Procedimientos primeros de la captura de paquetes de la infraestructura

Contenido

Introducción

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

Utilice el comando tcpdump

Esta sección proporciona los ejemplos que ilustran la manera en la cual utilizan al **comando tcpdump**.

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

La salida del **comando show interface** proporciona la información exacta sobre el nombre y el número de la interfaz que es actualmente funcionando.

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

> **Note**: Usted puede poder indica la cuenta específica del paquete en el comando anterior. Si usted no indica una cuenta específica del paquete, una captura continua se ejecuta sin el 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
```

> **Note**: Es el más fácil salvar el archivo, y después lo revisa. En este ejemplo, el servidor salva el archivo en la raíz de la estructura de directorios. Para ver los archivos, ingrese el **comando dir**.

Copie los archivos capturados a una ubicación exterior

Aquí están dos ejemplos que ilustran la manera de la cual capturó los archivos se copian a una ubicación que está fuera del servidor:

- En este ejemplo, el capturar archivo se copia a 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 capturar archivo se copia a un servidor TFTP con una dirección IP 5.6.7.8:

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

Paquetes de la captura como usuario raíz

Si usted desea capturas más granulares, registre en el CLI mientras que un *usuario raíz* después de que usted haya abierto una 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~]#
```

Capturas del usuario raíz del ejemplo

Aquí están tres ejemplos de las capturas que son tomadas por un usuario raíz:

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

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- En este ejemplo, todos los paquetes que se destinan al puerto **9991** se capturan y se escriben a un archivo llamado **test.pcap en el directorio de** /localdisk/ftp/:

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

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