Procedimentos principais da captura de pacote de informação da infraestrutura

Índice

Introdução

Este documento descreve o uso do comando CLI do **tcpdump** a fim capturar os pacotes desejados de um server da infraestrutura da prima de Cisco (PI).

Use o comando tcpdump

Esta seção fornece os exemplos que ilustram a maneira em que o **comando tcpdump** é usado.

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

A saída do **comando show interface** fornece a informação precisa sobre o nome e o número da relação que é atualmente em uso.

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

> **Note**: Você pode enlatar indica a contagem específica do pacote no comando precedente. Se você não indica uma contagem específica do pacote, uma captação contínua está executada sem o 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: É o mais fácil salvar o arquivo, e revê-o então. Neste exemplo, o server salvar o arquivo na raiz da estrutura do diretório. A fim ver os arquivos, inscreva o **comando dir**.

Copie os arquivos capturados a um lugar exterior

Estão aqui dois exemplos que ilustram a maneira em que capturou arquivos são copiados a um lugar que fosse fora do server:

- Neste exemplo, o arquivo de captura é copiado a um servidor FTP com um endereço IP de Um ou Mais Servidores Cisco ICM NT de **1.2.3.4**:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- Neste exemplo, o arquivo de captura é copiado a um servidor TFTP com um endereço IP 5.6.7.8:

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

Pacotes da captação como um usuário de raiz

Se você deseja umas captações mais granuladas, registre no CLI enquanto um *usuário de raiz* depois que você entrou como um *usuário 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~]#
```

Captações do usuário de raiz do exemplo

Estão aqui três exemplos das captações que são tomadas por um usuário de raiz:

- Neste exemplo, todos os pacotes que são destinados à porta **162 no** server PI são capturados:

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- Neste exemplo, todos os pacotes que são destinados à porta **9991** são capturados e escritos a um arquivo chamado **test.pcap no diretório de** /localdisk/ftp/:

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- Neste exemplo, todos os pacotes com um endereço IP de origem de **1.1.1.1** são capturados:

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