Procedimentos de Captura de Pacotes da Prime Infrastructure

Contents

Introduction

Este documento descreve o uso do comando CLI **tcpdump** para capturar os pacotes desejados de um servidor Cisco Prime Infrastructure (PI).

Usar o comando tcpdump

Esta seção fornece exemplos que ilustram a forma como o comando **tcpdump** é usado.

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

A saída do comando **show interface** fornece informações precisas sobre o nome e o número da interface que está em uso no momento.

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

> **Note**: Você pode indicar a contagem de pacotes específica no comando anterior. Se você não indicar uma contagem de pacotes específica, uma captura contínua será executada sem 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 mais fácil salvar o arquivo e depois revisá-lo. Neste exemplo, o servidor salva o arquivo na raiz da estrutura de diretório. Para visualizar os arquivos, digite o comando **dir**.

Copiar os arquivos capturados para um local externo

Aqui estão dois exemplos que ilustram a maneira como os arquivos capturados são copiados para um local fora do servidor:

- Neste exemplo, o arquivo de captura é copiado para um servidor FTP com um endereço IP de **1.2.3.4**:

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

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

Capturar pacotes como um usuário raiz

Se desejar capturas mais granulares, faça login na CLI como um usuário *raiz* depois de fazer login 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~]#
```

Exemplos de capturas de usuário raiz

Aqui estão três exemplos de capturas realizadas por um usuário raiz:

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

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- Neste exemplo, todos os pacotes destinados à porta **991** são capturados e gravados em um arquivo chamado **test.pcap** no **/localdisk/ftp/** diretory:

  ```
  [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
  ```