头等基础设施数据包捕获步骤

目录

[简介](#)
[请使用tcpdump命令](#)
[复制获取文件到一个外部位置](#)
[获取数据包作为Root用户](#)
[示例Root用户捕获](#)

简介

本文描述CLI命令使用的**tcpdump**为了获取从Cisco最初基础设施(PI)服务器的所需的信息包。

请使用tcpdump命令

此部分提供说明方式**tcpdump命令**使用的示例。

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

show interface命令提供准确的信息的输出关于正在使用中的接口名称和编号的。

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

> **Note**:您能能指示在前面的命令的特定包计数。如果不指示特定包计数，一个连续捕获运行没有限制。

```
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**:保存文件，然后查看它是最容易的。在本例中，服务器保存在目录结构的根的文件。为了查看文件，输入**dir命令**。

复制获取文件到外部位置

这是说明方式获取文件复制到位置是在服务器外面的两示例：

- 在本例中，捕获文件复制对一个FTP服务器用1.2.3.4的IP地址：

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- 在本例中，捕获文件复制对与IP地址5.6.7.8的一TFTP server ：

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

捕获数据包作为Root用户

如果希望更加粒状的捕获，请登录CLI作为*root用户*，在您登陆作为*管理员用户后*。

```
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~]#
```

示例Root用户捕获

这是由root用户采取捕获的三示例：

- 在本例中，被注定到端口162 PI服务器的所有数据包捕获：

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- 在本例中，被注定到端口9991的所有数据包捕获并且写入到呼叫在/localdisk/ftp/目录的test.pcap的文件：

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- 在本例中，有1.1.1.1源IP地址的所有数据包捕获：

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