Prime基础设施数据包捕获过程

目录

简介

本文档介绍使用tcpdump CLI命令从Cisco Prime基础设施(PI)服务器捕获所需数据包。

使用tcpdump命令

本节提供示例，说明使用tcpdump命令的方式。

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

show interface命令的输出提供了有关当前使用的接口名称和编号的精确信息。

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

> **注意**：您可以在上一命令中指示特定包计数。如果未指示特定包计数，则运行连续捕获，无限制。

```
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
```

> **注意**：保存文件并查看最简单。在本例中，服务器将文件保存在目录结构的根目录中。要查看文件，请输入dir命令。

将捕获的文件复制到外部位置

以下两个示例说明捕获文件复制到服务器外部位置的方式：

- 在本示例中，捕获文件被复制到IP地址为1.2.3.4**的FTP服务器**:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- 在本示例中，捕获文件被复制到IP地址为5.6.**7.8的TFTP服务器**:

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

以根用户身份捕获数据包

如果需要更精细的捕获，请在以管理员用户*身份登录*后，以根用户*身份*登录*CLI*。

```
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~]#
```

根用户捕获示例

以下是根用户捕获的三个示例：

- 在本示例中，将捕获发往PI服务器上端**口162**的所有数据包：

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- 在本示例中，发往端口9991的所有数据包都会被捕**获并**写入/localdisk/ftp/目录**中名为** test.pcap**的文件中：**

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- 在本示例中，将捕获源IP地址为1.1.**1.1的所有数**据包：

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