Prime Infrastructure Packet Capture-Verfahren

Inhalt

Einführung

In diesem Dokument wird die Verwendung des Befehls **tcpdump** CLI beschrieben, um die gewünschten Pakete von einem Cisco Prime Infrastructure (PI)-Server zu erfassen.

Verwenden des Befehls tcpdump

In diesem Abschnitt finden Sie Beispiele, die veranschaulichen, wie der Befehl **tcpdump** verwendet wird.

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

Die Ausgabe des Befehls **show interface** liefert präzise Informationen über den aktuell verwendeten Schnittstellennamen und die Nummer.

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

> **Hinweis**: Sie können die Anzahl der Pakete im vorherigen Befehl angeben. Wenn Sie keine bestimmte Paketanzahl angeben, wird eine fortlaufende Erfassung ohne Begrenzung ausgeführt.

```
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
```

Hinweis: Sie können die Datei am einfachsten speichern und dann überprüfen. In diesem Beispiel speichert der Server die Datei im Stammverzeichnis der Verzeichnisstruktur. Um die Dateien anzuzeigen, geben Sie den Befehl **dir ein**.

Kopieren der erfassten Dateien an einen externen Speicherort

Hier sind zwei Beispiele, die veranschaulichen, wie aufgezeichnete Dateien an einen Speicherort außerhalb des Servers kopiert werden:

- In diesem Beispiel wird die Erfassungsdatei auf einen FTP-Server mit der IP-Adresse **1.2.3.4** kopiert:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- In diesem Beispiel wird die Erfassungsdatei auf einen TFTP-Server mit der IP-Adresse **5.6.7.8** kopiert:

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

Erfassen von Paketen als Stammbenutzer

Wenn Sie detailliertere Aufnahmen wünschen, melden Sie sich als *Root*-Benutzer bei der CLI an, nachdem Sie sich als *Admin*-Benutzer angemeldet haben.

```
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~]#
```

Beispiel für Root-Benutzeraufzeichnungen

Hier sind drei Beispiele für von einem Root-Benutzer aufgezeichnete Aufnahmen:

- In diesem Beispiel werden alle Pakete, die für Port **162** auf dem IP-Server bestimmt sind, erfasst:

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- In diesem Beispiel werden alle Pakete, die für den Port **9991** bestimmt sind, erfasst und in eine Datei mit dem Namen **test.pcap** im **/localdisk/ftp/**directory geschrieben:

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- In diesem Beispiel werden alle Pakete mit der Quell-IP-Adresse **1.1.1.1** erfasst:

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