Packet Capture Procedures voor Prime-infrastructuur

Inhoud

Inleiding

Dit document beschrijft het gebruik van de opdracht **TCP-pomp** CLI om de gewenste pakketten op te nemen van een Cisco Prime-server (IP).

Gebruik de opdracht Temperatuur

Dit deel geeft voorbeelden die de manier illustreren waarop de opdracht **ingedrukt** wordt.

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

De output van de opdracht **show interface** geeft nauwkeurige informatie over de interfacenaam en het nummer dat momenteel in gebruik is.

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

> **Opmerking:** U kunt de specifieke pakkettelling in de vorige opdracht aangeven. Als u geen specifieke pakkettelling aangeeft, wordt een continue opname zonder limieten uitgevoerd.

```
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
```

Opmerking: Het is het eenvoudigst om het bestand op te slaan en het vervolgens te bekijken. In dit voorbeeld, slaat de server het bestand op in de wortel van de folder structuur. Typ de opdracht **dir** om de bestanden te bekijken.

De opgenomen bestanden naar een externe locatie kopiëren

Hier zijn twee voorbeelden die de manier illustreren waarop de opgenomen bestanden worden gekopieerd naar een locatie die buiten de server valt:

- In dit voorbeeld, wordt het opnamebestand gekopieerd naar een FTP-server met een IP-adres van **1.2.3.4**:

  ```
  copy disk:/test-capture.pcap ftp://1.2.3.4/
  ```
- In dit voorbeeld wordt het opnamebestand gekopieerd naar een TFTP-server met een IP-adres **5.6.7.8**:

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

Packet als Root-gebruiker opnemen

Als u meer korrelige opnamen wilt hebben, logt u als basisgebruiker in op de CLI nadat u als *beheerder* hebt aangemeld.

```
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~]#
```

Voorbeelden van ruitgebruikersopnamen

Hier zijn drie voorbeelden van opnamen die door een root gebruiker zijn gemaakt:

- In dit voorbeeld worden alle pakketten die voorzien zijn van poort **162** op de IP server opgenomen:

  ```
  [root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
  ```
- In dit voorbeeld worden alle pakketten die bedoeld zijn om poort **991** te **openen** opgenomen en geschreven naar een bestand dat **test.pcap** wordt genoemd in de **/localdisk/ftp/**folder:

  ```
  [root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
  ```
- In dit voorbeeld worden elke pakketten met een bron IP-adres van **1.1.1** opgenomen:

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