互連行動體驗上的封包擷取(CMX)

目錄

簡介

Connected Mobile Experience(CMX)10.xCLI(LAN(WLC)CMX)NMSP

需求

- CMX(CLI)
- Wireshark

使用TCPDUMP進行捕獲

TCPDUMP是一種資料包分析器，用於顯示CMX伺服器上傳輸和接收的資料包。它是網路/系統管理員的分析和故障排除工具。該資料包內建在CMX伺服器上，可以在其中檢視資料包的原始資料。

以「cmxadmin」使用者身份運行tcpdump將失敗，錯誤如下：（需要「root」訪問許可權）

```
In this example, tcpdump is attempted to be run as a 'cmxadmin' user.

[cmxadmin@laughter ~]$ tcpdump -i eth0 port 16113
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
```

以「cmxadmin」使用者身份通過SSH或控制檯登入到CLI後，切換到「root」使用者。

```
[cmxadmin@laughter ~]$ su - root
Password:
[root@laughter ~]#
```

使用正確的介面

記下將擷取封包的介面。可以使用「ifconfig-a」取得

In this example, 10.10.10.25 is the IP address of CMX server and 'eth0' is the interface it's tied to on the server.

```
[cmxadmin@laughter ~]$ ifconfig -a eth0      Link encap:Ethernet  HWaddr 00:50:56:A1:38:BB
          inet addr:10.10.10.25  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: 2003:a04::250:56ff:fea1:38bb/64 Scope:Global
          inet6 addr: fe80::250:56ff:fea1:38bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32593118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3907086 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3423603633 (3.1 GiB)  TX bytes:603320575 (575.3 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1136948442 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1136948442 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:246702302162 (229.7 GiB)  TX bytes:246702302162 (229.7 GiB)

[cmxadmin@laughter ~]$
```

捕獲資料包

This example captures and displays all packets that are sourced from port - 16113 and enter the CMX server on the eth0 interface.

```
[root@laughter ~]# tcpdump -i eth0 src port 16113 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes 09:50:29.530824 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 983381312:983382645, ack 2483597279, win 191, options [nop,nop,TS val 1792647414 ecr 1148435777], length 1333 09:50:31.507118 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [.], seq 1333:2715, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650], length 1382 09:50:31.507186 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 2715:2890, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650], length 175 09:50:33.483166 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 2890:4239, ack 1, win 191, options [nop,nop,TS val 1792648402 ecr 1148439626], length 1349 09:50:35.459584 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 4239:5396, ack 1, win 191, options [nop,nop,TS val 1792648896 ecr 1148441603], length 1157 ^C 5 packets captured 5 packets received by filter 0 packets dropped by kernel [root@laughter ~]#
```

將輸出寫入檔案

In this example, tcpdump would capture packets that are from 10.10.20.5 received on it's eth0 interface and write it to a file named TEST_NMSP_WLC.pcap.

```
[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.5 -w TEST_NMSP_WLC.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C7 packets captured
7 packets received by filter
0 packets dropped by kernel
[root@laughter cmxadmin]#
```

一旦檔案準備就緒，您就需要將.pcap檔案從CMX提取到電腦中，以便使用更舒適的工具（如wireshark）進行分析。您可以使用任何SCP應用程式來完成此操作。例如，在Windows中，WinSCP應用程式將允許您使用SSH憑據連線到CMX，然後您可以瀏覽檔案系統並找到剛建立的

.pcap檔案。要查詢當前路徑，請在運行tcpdump後鍵入「pwd」以瞭解檔案儲存的位置。

捕獲特定數量的資料包

如果需要特定數量的資料包計數，則使用 — c選項完全過濾該計數。

```
[root@laughter ~]# tcpdump -Z root -i eth0 -c 5 src 10.10.20.5 -w CMX_WLC_Capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
5 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@laughter ~]#
```

其他篩選選項

```
[root@laughter cmxadmin]# tcpdump -i eth0 dst 10.10.20.5 (filtered based on destination IP
address)
[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.4 (filtered based on Source IP address)

[root@laughter cmxadmin]# tcpdump -i eth0 port 80  (filtered for packets on port 80 in both
directions)
[root@laughter cmxadmin]# tcpdump -i eth0 port 443  (filtered for packets on port 443 in both
directions)
```

寫入檔案的捕獲將儲存在伺服器上的當前目錄中，並且可以通過Wireshark複製出來進行詳細檢視。