Jabber訪客伺服器上的封包擷取

目錄

簡介

本檔案介紹如何從Jabber Guest Server擷取封包擷取。

必要條件

需求

思科建議您瞭解以下主題：

- Jabber Guest必須能夠訪問Internet以下載程式包。
- 在PC上安裝WinSCP軟體以收集捕獲。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Jabber Guest版本10.5和10.6
- WinSCP軟體

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題：如何從Jabber Guest Server獲取資料包捕獲？

解決方案

步驟1.

Jabber Guest伺服器必須能夠訪問Internet，以便從Internet下載軟體包。在使用Web代理的情況下，請按照該過程允許Jabber Guest上的CentOS使用Web代理下載包。

請參閱連結https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html以按照以下步驟操作。

確保Jabber Guest Server可以下載軟體包後，請繼續執行步驟2。

步驟2.

使用安全套接字主機(SSH)根憑證登入到Jabber Guest伺服器，並運行**yum search tcpdump**命令以查詢最新版本的tcpdump。

```
[root@jabberguest ~]# yum search tcpdump
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.host-engine.com
 * extras: centos.mirror.nac.net
 * updates: centos.arvixe.com
============================================================================ N/S Matched: tcpdump =====
tcpdump.x86_64 : A network traffic monitoring tool

  Name and summary matches only, use "search all" for everything.
[root@jabberguest ~]#
```

步驟3.

運行**yum install tcpdump**命令，在Jabber Guest Server上安裝tcpdump軟體包。

```
[root@jabberguest ~]# yum install tcpdump
Loaded plugins: fastestmirror
Setting up Install Process
Determining fastest mirrors
 * base: centos.aol.com
 * extras: centos.mirror.ndchost.com
 * updates: centos.mirror.nac.net
base                                                     | 3.7 kB     00:00
extras                                                   | 3.4 kB     00:00
extras/primary_db                                        |  31 kB     00:00
updates                                                  | 3.4 kB     00:00
updates/primary_db        50% [=======-       ]  0.0 B/s | 2.0 MB     --:-- ETA
```

步驟4.

系統通過多個提示向您傳送消息。在每個元件上輸入**y**以驗證每個提示。

步驟5.

Tcpdump現在再次可用於從Jabber Guest Server捕獲資料包。

```
[root@jabberguest ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:44:54.328431 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 1089242520:1089242728, ack 1202666623, win 20832, length 208
11:44:54.329007 IP jabberguest.havogel.com.50843 > ad.havogel.com.domain: 15118+ PTR? 66.25.0.14.in-addr.arpa. (41)
11:44:54.384348 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 4294967232:208, ack 1, win 20832, length 272
11:44:54.388191 IP 14.0.25.66.60858 > jabberguest.havogel.com.ssh: Flags [.], ack 208, win 64384, options [nop,nop,sack 1 {4294967232:208}], length 0
11:44:54.579286 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:54.656970 ARP, Request who-has 14.80.94.11 tell 14.80.94.1, length 46
11:44:54.660995 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.237405 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:55.579320 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:55.660815 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.915532 ARP, Request who-has 14.80.94.104 tell 14.80.94.1, length 46
11:44:55.921206 ARP, Request who-has 14.80.94.150 tell 14.80.94.1, length 46
11:44:56.102066 ARP, Request who-has 14.80.94.66 tell 14.80.94.56, length 46
11:44:56.113541 ARP, Request who-has 14.80.94.48 tell 14.80.94.220, length 46
11:44:56.234761 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:56.281613 ARP, Request who-has 14.80.94.101 tell 14.80.94.1, length 46
```

您可以使用**tcpdump -w TAC.pcap**命令運行tcpdump並將捕獲寫入.pcap檔案。

步驟6.

您可以使用WinSCP從Jabber訪客伺服器收集檔案。系統會開啟產品上的增強功能，以從Web GUI獲取資料包捕獲，並在以下位置對其進行跟蹤：

https://tools.cisco.com/bugsearch/bug/CSCuu99856/?reffering_site=dumpcr