Jabber访客服务器上的数据包捕获

目录

简介

本文档介绍如何从Jabber访客服务器捕获数据包。

先决条件

要求

Cisco 建议您了解以下主题：

- Jabber访客必须能够访问互联网才能下载软件包。
- 安装在PC上以收集捕获的WinSCP软件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Jabber访客版本10.5和10.6
- WinSCP软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题：如何从Jabber访客服务器捕获数据包？

解决方案

步骤1:

Jabber Guest服务器必须能够访问Internet，才能从Internet下载软件包。如果使用Web代理，请按照以下步骤操作：允许Jabber Guest上的CentOS使用Web代理下载包。

请参阅链接https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html，按照此步骤操作。

确保Jabber Guest Server可以下载软件包后，请继续步骤2。

第二步：

使用安全套接字主机(SSH)根凭证登录Jabber Guest服务器，并运行**yum search tcpdump**命令以查找最新版本的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 ~]#
```

第三步：

运行**yum install tcpdump** 命令以在Jabber Guest Server上安装tcpdump软件包。

```
[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
```

第四步：

您会通过多个提示发送。在每个组件上输入**y**以验证每个提示。

第五步：

现在，Tcpdump可再次用于从Jabber访客服务器捕获数据包。

```
[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命令运行tcpdump并在.pcap文**件上写入捕获**内容。

第六步：

您可以使用WinSCP从Jabber访客服务器收集文件。将打开产品上用于从Web GUI获取数据包捕获的增强功能，并在以下位置进行跟踪：

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