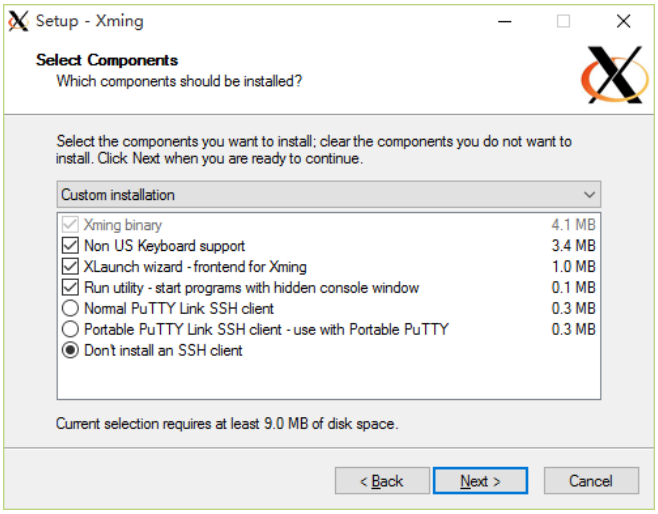
Linux Server版下如何使用Wireshark进行抓包

wangjun 2016-01-05 发表

Ubuntu Server版缺省安装后，由于不包含Wireshark抓包软件，导致无法对收发报文进行抓包分析，无法快速准确的定位问题。
通过以下命令成功安装Wireshark后，发现无法正常运行Wireshark 。
apt-get update apt-get install wireshark

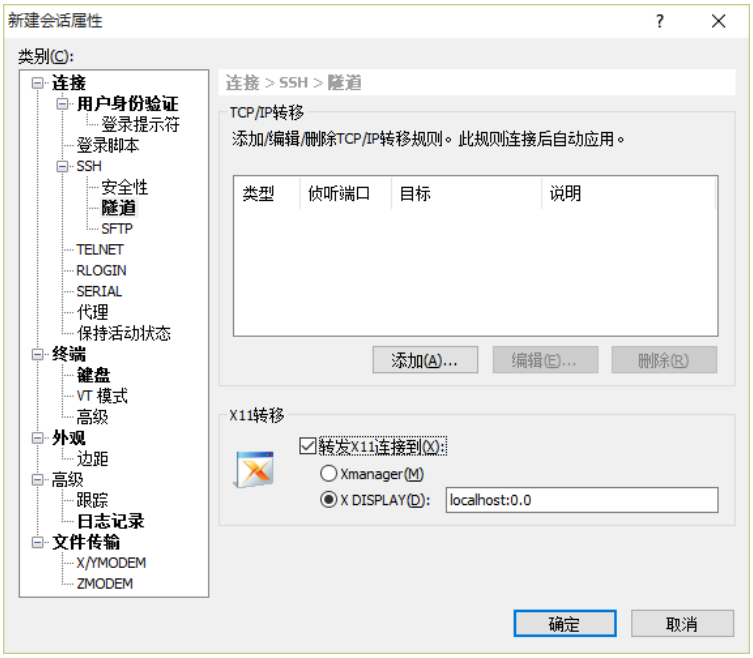
在终端上启动Wireshark软件出现以下错误提示，软件无法正常运行。
ubuntu@ubuntu:~$ sudo wireshark
error: XDG_RUNTIME_DIR not set in the environment.
(wireshark:1246): Gtk-WARNING **: cannot open display:
由于Linux Server版本的缺省安装为命令行界面，不包含GUI组件，而Wireshark运行需要GUI的支持才可以，导致Wireshark无法启动。
解决方法有两个：
方法1. 在Linux安装GUI环境来运行Wireshark
方法2. 通过SSH连接的X11转移功能来运行Wireshark
方法1需要在服务器上安装额外的GUI环境，对服务器的环境改变改变较大，并且安装的GUI也带来额外的系统资源的消耗。如果只是为了抓包而增加服务器的资源占用，有点得不偿失，因此不是我们的首选方案。
因此对于方法1不展开讲述，下面重点讲如何通过方法2来实现。

1、安装Xming
首先在SSH客户端所在的电脑上下载并安装Xming软件。Xming X Server for Windows



如果已经安装过SSH客户端软件，在安装过程中可以选择不安装PuTTY软件。安装成功后，在Windows的任务管理器中能够看到Xming Server的图标。

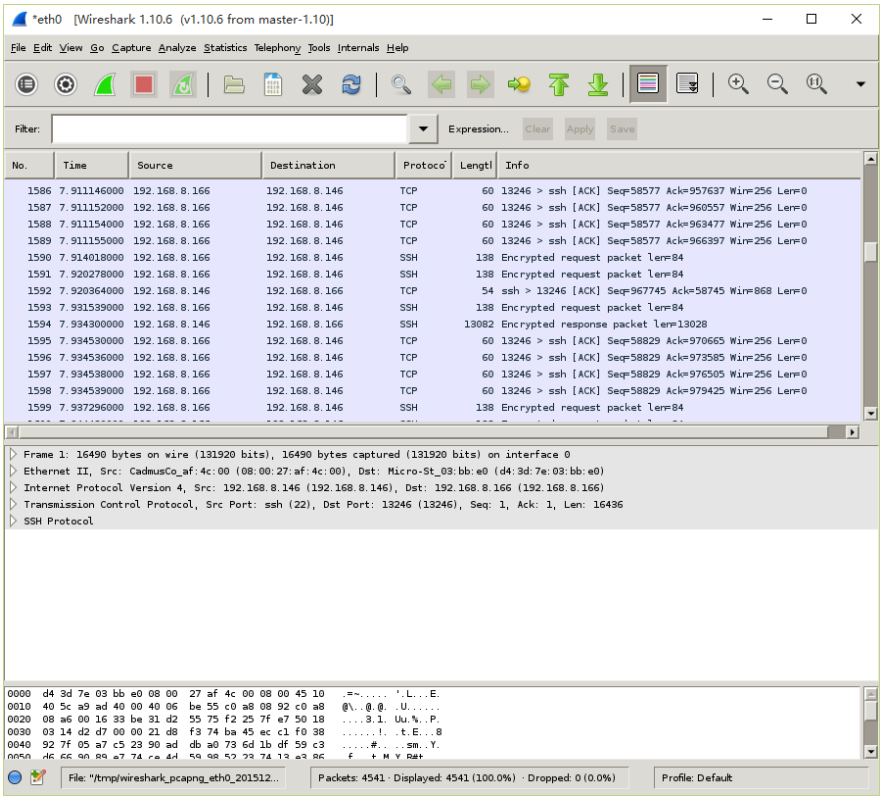
2、设置Xshell，启用X11转发功能
在Xshell中对创建的SSH会话进行如下设置：“连接>SSH>隧道”的“X11转移”，勾选“X DISPLAY”，参数无需修改。



重新连接SSH后，在终端中执行

sudo wireshark

我们就能看到熟悉的图形界面了，Wireshark的操作和Windows下完全一致。这样就可以根据我们的要求来进行报文抓取和分析了。捕获的数据报文保存在服务器上，可以通过SFTP方式下载到本地。



1、以上以Ubuntu 12.04.3 Server版本为例进行说明，其他版本的Linux也一样适用。

2、对于习惯适用PuTTY客户端的，只需要在PuTTY的设置中使能X11转发功能即可。

3、通过X11转发的方式，对于服务器不用安装GUI组件，减少了服务器的资源消耗是推荐的首选方法。

4、需要以sudo的方式来启动Wireshark，否则会由于没有权限导致无法进行抓包。