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

🗙 Setup - Xming -	_		Х
Select Components Which components should be installed?		ζ	\mathbf{X}
Select the components you want to install; clear the components you do install. Click Next when you are ready to continue.	not wa	ant to	
Custom installation		~]
Z Xming binary		4.1 MB	1
Non US Keyboard support		3.4 MB	
XLaunch wizard - frontend for Xming		1.0 MB	
Run utility - start programs with hidden console window		0.1 MB	
Normal PuTTY Link SSH client		0.3 MB	
Portable PuTTY Link SSH client - use with Portable PuTTY Ont install an SSH client		0.3 MB	
Current selection requires at least 9.0 MB of disk space.			1
< <u>B</u> ack <u>N</u> ext >		Can	cel

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Window s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。

新建会话属性		?	×
类别(C):			
 □· 注接 □· 用户身份验证 □· 登录提示符 □· 登录脚本 □· SSH 	注接 > 55H > 隧道 TCP/匹转移 添加/编辑/删除尔CP/匹转移规则。此规则注接后自动应用	0	
安全性 隆道 SFTP TELNET RLOGIN SERIAL 代理 保持活訪状态	类型 位听端口 目标 说明		
□- 终端 雑盘 	添加(A) 编辑(E) X11转移	刪除(R)	
 小观 → 边距 □→ 高级 →	✓結发X11连接到(X): ○ Xmanager(M) ④ X DISPLAY(D): localhost:0.0		
₩ XHTRM X/YMODEM ZMODEM	确定	取消	Ť

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。