基于Python实现的抓包分析软件

Expiredlove
发布日期: 1 年前 浏览量: 1747 收藏:4

评分：★ ★ ★ ★ ★ ★ ★ ★ ☆ ☆

Expiredlove

发送私信

你最美丽的时光陪我度过那些年

7 文章数　5 评论数

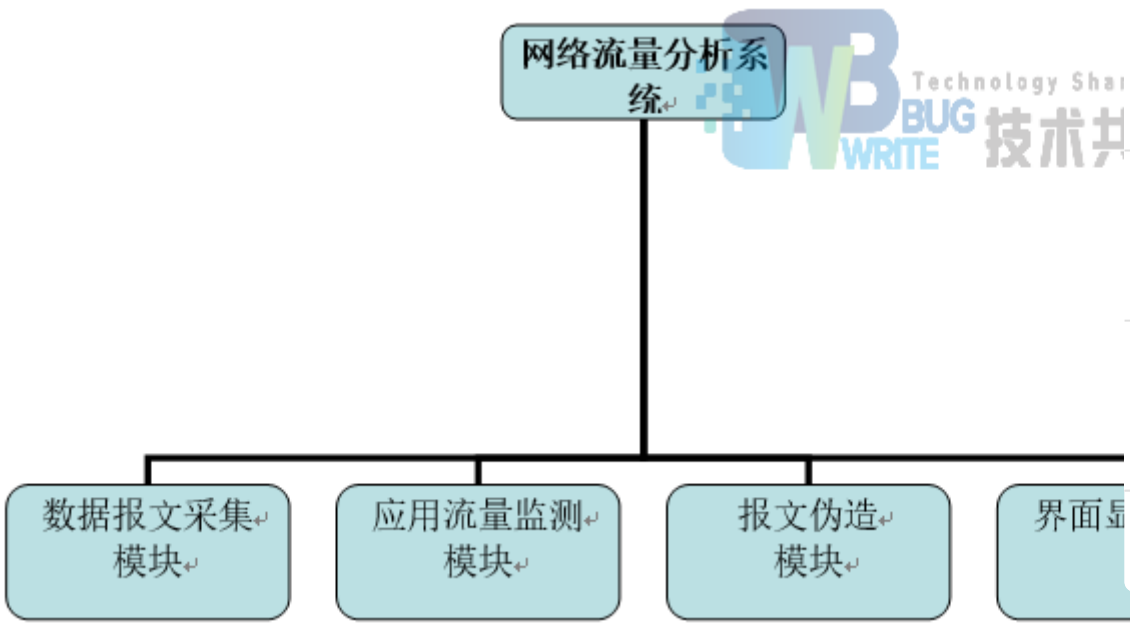
一、简介

这是一个学习模仿WireShark的抓包软件。可以的功能有：侦听、解析、构造数据包等。其中还包括扩展功能：流量监 of Death）。软件目前支持解析：IP、IPv6、ARP、TCP、UDP、ICMP、ICMPv6、SSDP、HTTP、TLS。

二、主要功能

- 侦听指定网卡或所有网卡，抓取流经网卡的数据包
- 解析捕获的数据包每层的每个字段，查看数据包的详细内容
- 可通过不同的需求设置了BPF过滤器，获取指定地址、端口或协议等相关条件的报文
- 针对应用进行流量监测，监测结果实时在流量图显示，并可设置流量预警线，当流量超过预警线时自动报警
- 提供了以饼状图的形式统计ARP、TCP、UDP、ICMP报文，以柱状图的形式统计IPv4、IPv6报文
- 可将抓取到的数据包另存为pcap文件，并能通过打开一个pcap文件对其中的数据包进行解析
- 可逐层逐字段构造数据包，实现自定义数据包发送

三、主要模块



数据报文采集模块：完成网络接口数据的捕获、解析，可以根据用户定义条件组合来进行捕获，如只监视采用TCP或UDP协议的数据包，也可以监视用户希望关注的相关IP地址的数据包，同时完成数据封包日志记录，提高了系统的灵活性。此外，对IP类型、ARP、TCP、UDP、ICMP的数量进行统计。

应用流量监测模块：获取当前正在运行的应用进程，用户可选择一个应用进行流量监测，获取应用中流量信息，同时对一些常见的入侵攻击特征进行判断，如根据源目的地址是否相同判断Land攻击、IP头部长度是否过长判断ping拒绝服务攻击，并发出预警。

报文伪造模块：可以自行构造Ether、IP、TCP、UDP、ICMP、ARP报文，并选择send()、sendp()、sr()、srl()、srloop()五种方式发送报文以实现简单攻击或对TCP/IP进行调试。

界面显示模块：设计系统主窗口即数据报文采集界面、应用流量监测界面、报文伪造界面。并完成报文统计图的显示，流量图的显示。

四、源代码结构

- **img**
  存放程序中使用的背景和图标。

最近文章

基于JavaScript实现的地铁交通网络管理和线路查询系统
21 天前 (0)

基于Qt实现的B-树演示程序
17 天前 (0)

基于Python实现的抓包分析软件
1 年前 (1)

基于OpenCV实现的自动扫雷机
1 年前 (1)

基于C#实现的TPS和B样条人脸变形系统
1 年前 (3)

基于JSP实现的学生成绩管理系统
2 年前 (2)

浏览更多