网络流量可视化专家

(FlowView)

使用说明书

1 概述

FlowView 具有最小巧的报文分析和网络审计引擎（只有 200K），该引擎还具有跨平台的特性，可以在 windows、Linux 和 VxWorks 下运行，在 Linux 下配合网卡零拷贝可以实现更高性能的报文分析。

1.1 功能介绍

网路流量分析专家主要具有以下功能：

1) 支持多种协议
   支持各种协议封转，支持 PPPOE、VALN、MPLS、GRE 等封装

2) 网页分析
   截获用户浏览网页的 URL 并进行分类，并能对指定的 URL 类别进行页面还原
   截获用户通过网页发送的信息并进行还原
   统计用户访问的 HOST 排名
   截获常用搜索引擎的搜索关键字

3) 电子邮件
   能截获 SMTP 发送邮件的接收者、发送者、标题、正文及附件，并能将发送的邮件还原为 eml 文件
   能截获 POP3 收邮件的接收者、发送者、标题、正文及附件，并能将接收的邮件还原为 eml 文件

4) WebMail 邮件
   对于常用的 WebMail 邮件采用智能识别的方法，对于诸如接收者、发送者、标题、正文之类的关键字进行分析，并能重组为 eml 文件

5) 文件传输
   能截获 Ftp 的登录账号、操作类型、文件信息等

6) QQ 聊天
   能截获 QQ 的账号及其状态，如果知道 QQ 密码的情况下，可以对 QQ 聊天内容进行还原

7) MSN 聊天
   能截获 MSN 的账号以及好友列表、状态以及聊天内容。

8) 实时流量分析
   采用 DPI 和 DFI 相结合的进行协议识别， 能识别的协议主要下面几类
   标准协议 SMTP，POP3，IMAP，Telnet，FTP，DNS，DHCP，TFTP，SNMP，

NFS，NTP
P2P 下载 迅雷、BT、eDonkey，Poco、Vagaa、超级旋风，Flashget、汉魅等协议
P2P 视频 迅雷看看、PPStream，PPLive，QQ 影音、QVod，PPFilm、飞速土豆
即时通信 QQ、MSN、AIM、淘宝、飞信
网络游戏 魔兽，奇迹世界、巨人、征途

1.2 安装

解压后在 FlowView 文件夹下的 bin 为应用程序所在的目录，如果没有安装 winpcap,首选必须安装目录下的 WinPcap_4_1_2.exe 程序。

程序有四部分组成
1）报文分析引擎 engine.exe
用于报文捕捉、流量分析、内容审计

2）数据记录 dblog.exe
用于数据记录以及一些统计功能

3）查看工具 flowview.exe
对记录的数据进行查看和查询，以及启动和停止报文分析引擎以及数据

4）记录工具
数据库 mysql-nt.exe

1.3 版本历史

V0.2.2.9 20111214
Engine.exe 0.2.2.9
Dblog.exe 0.2.2.9
Flowview.exe 0.2.2.9
发布第一版

2 使用说明

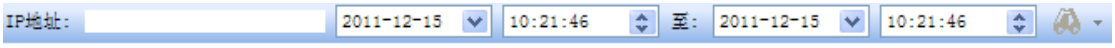
2.1 启动

执行 start.cmd 脚本，依次启动 mysql-nt.exe、Engine.exe、DbLog.exe,
然后可以通过 flowview.exe 来查看记录数据了，登陆用户名缺省为 admin,密码缺省为 admin
如果需要重启引擎，执行 restart.cmd 重启程序
关掉引擎，执行 stop.cmd

2.2 工具条

 选择监控的网卡，修改了网卡后，调用 restart.cmd 程序将引擎重启。

 第一个按钮表示启动引擎和数据记录，第二个按钮表示停止引擎和数据记录。



这个用户记录查询，可以根据 IP 地址、截获时间进行查询，对于有些协议可以对截获内容进行查询  下拉框会弹出内容查询按钮。

2.3 协议查看

协议查看

现在支持的协议有网页浏览、电子邮件、文件传输、远程访问、MSN 和 QQ 聊天等协议。操作比较简单，不再赘述。

3 建议

如果您对软件有什么建议或项目合作，请发邮件给我，flowview@163.com