**《网络被攻击过程图形化显示系统》**

**需求规格说明书**

**修订表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **版本** | **修订人** | **修订章节与内容** | **修订日期** |
| 1 | 1.0 | 张海汀 | 初版规格说明书 | 2020/9/8 |
| 2 | 1.1 | 张海汀 | 增加功能需求 | 2020/9/11 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

一、引言

1.目的

2.范围

二、系统定义

三、应用环境

四、功能规格

1.系统功能列表

2.读入数据

3.分析网络监控数据

4.图形化显示

五、其他需求

1.性能需求

2.扩展需求

六、产品提交

七、其他

一、引言

1.目的

本文档是网络被攻击过程图形化显示系统的需求规格说明书，旨在说明本图形化显示系统的需求规格，并作为用户验收参考以及开发团队开发过程中的参考。

2.范围

本文档为系统的功能需求描述，包括了系统总体设计描述以及各个功能模块的详细描述。

二、系统定义

本系统需要能够读入用户指定的.pcap或.csv格式的大数据包。如果包内数据是适当格式的网络监控数据，则本系统能够对数据进行分析，而后生成由节点构成的网络环境。系统能够根据流量关系，计算攻击过程，而后图形化显示网络被攻击过程。

三、应用环境

Windows 10计算机系统。

**四、功能规格**

1.系统功能列表

|  |  |  |
| --- | --- | --- |
| 功能类别 | 功能名称 | 一般过程描述 |
| 读入数据 | 读入PCAP包 | 读入用户指定路径的PCAP包 |
| 读入EXCEL | 读入用户指定路径的.csv文件 |
| 分析网络监控数据 | 输入验证 | 判断读入的包是否是适当格式的网络监控数据 |
| 分析数据 |  |
| 生成网络环境 | 生成由节点构成的网络环境 |
| 计算攻击过程 | 根据流量关系计算攻击过程 |
| 图形化显示 | 读入数据包 | 弹出窗口使用户可以指定读入数据包的路径 |
| 显示网络环境 | 显示数据包的整体网络环境 |
| 显示攻击过程 | 显示数据包内的指定攻击过程 |
| 选择时间范围 | 选择时间范围内的数据进行图形化显示 |
| 放大 | 放大图形显示 |
| 缩小 | 缩小图形显示 |
| 变速显示 | 增加/减少单位时间内显示的单位时间数流量 |
| 按端口显示 | 显示端口之间的数据流动 |
| 选择IP地址显示 | 显示指定IP地址范围内的节点间数据流动 |
| 选择攻击 | 选择显示指定攻击的攻击过程 |
| 关闭 | 关闭当前数据包的图形化显示 |

2.读入数据

基本描述：

读入指定路径的PCAP包或EXCEL表。如果是PCAP包，转向PCAP包分析环节；如果是EXCEL，转向EXCEL分析环节。

3.分析网络监控数据

3.1 输入验证

判断读入的包是否是适当格式的网络监控数据、能够用于分析。如果不是，返回报错。

3.2 生成网络环境

生成由节点和链路连接构成的网络环境。

3.3 计算攻击过程

根据网络流量数据计算攻击过程。至少实现DOS攻击的分析和显示。

4.图形化显示

实现一个图形界面，能够导入数据包。如果导入的数据包不能处理，弹出报错窗口；否则弹出图形化显示窗口。默认显示网络环境的图形化显示，可以指定显示的时间范围；同时界面可以选择展示单个指定的攻击过程，对于这个攻击过程可以指定显示时间范围内的攻击。

4.1 放大/缩小

图形放大到最大时可以显示节点数据流的所有信息、包括时间、报文长度、报文内容、协议等，缩小后逐渐减少显示信息。

4.2 变速显示

正常速度下每秒显示一秒内网络环境数据流动，可以加速，使最高一秒内显示16秒内网络环境数据流动。

**五、其他需求**

1.性能需求

应当支持5000以上节点的分析和显示

应当支持变速显示

2.扩展需求

支持显示流量大小

六、产品提交

应当提交一份可在Windows 10计算机操作系统上使用的安装包，同时提交用户使用手册。

七、其他

用例图：

