**概要设计说明书**

**1 引言**

1.1编写目的

网络攻击图系统概要设计说明书编写的目的是说明对程序系统的设计考虑，包括程序系统的基本处理，包括流程、程序系统的组织结构、模块划分、功能分配接口设计、运行设计、数据结构设计和出错处理设计等。为程序的详细设计提供基础。

1.2背景

待开发系统名称：网络攻击图系统

项目提出者：赵小林老师

项目开发者：汪一帆、冯蒙博、申志宇、主文浩、张明熙、张雅彬、胡港

用户：网络安全分析人员

1.3定义

CVE：CVE 的英文全称是“Common Vulnerabilities & Exposures”通用漏洞披露。CVE就好像是一个字典表，为广泛认同的[信息安全](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/339810" \t "https://baike.baidu.com/item/CVE/_blank)漏洞或者已经暴露出来的弱点给出一个公共的[名称](https://baike.baidu.com/item/%E5%90%8D%E7%A7%B0/6546057" \t "https://baike.baidu.com/item/CVE/_blank)。

1.4参考资料

【1】https://www.sohu.com/a/156772659\_822985 什么是网络攻击图

【2】[汪渊](http://common.wanfangdata.com.cn/common/getAuthorUrl.do?&authorName="%E6%B1%AA%E6%B8%8A"" \t "http://d.wanfangdata.com.cn/thesis/_blank),[蒋凡](http://common.wanfangdata.com.cn/common/getAuthorUrl.do?&authorName="%E8%92%8B%E5%87%A1"" \t "http://d.wanfangdata.com.cn/thesis/_blank),[陈国良](http://common.wanfangdata.com.cn/common/getAuthorUrl.do?&authorName="%E9%99%88%E5%9B%BD%E8%89%AF"" \t "http://d.wanfangdata.com.cn/thesis/_blank).[基于图论的网络安全分析方法研究与应用](http://d.wanfangdata.com.cn/periodical/xxwxjsjxt200310032" \t "http://d.wanfangdata.com.cn/thesis/_blank)[J].

【3】王会梅，鲜明，王国玉.[基于扩展网络攻击图的网络攻击策略生成算法](http://d.wanfangdata.com.cn/Periodical/dzkxxk201112036" \t "https://xueshu.baidu.com/usercenter/paper/_blank)

**2[总体设计](https://baike.baidu.com/item/%E6%80%BB%E4%BD%93%E8%AE%BE%E8%AE%A1" \t "https://baike.baidu.com/item/%E6%A6%82%E8%A6%81%E8%AE%BE%E8%AE%A1%E8%AF%B4%E6%98%8E%E4%B9%A6/_blank)**

2.1 需求规定

2.1.1功能性需求

1、读入PCAP包或EXCEL大数据

读入数据是数据分析的起点，对于我们的网络攻击图系统，要求输入的内容一般分为两部分：需要分析的数据，以及判定数据是否异常，网络是否存在漏洞的判定条件。

我们的系统必须要做到能够支持读取EXCEL大数据或者读取PCAP包当中的数据。

2、分析网络监控数据

系统必须能够自动对导入的数据进行扫描分析，并且能够分辨出正常情况下不同主机之间的数据传输情况与存在网络安全漏洞情况下数据传输情况的区别。

3、输入被攻击节点的漏洞情况，根据流量和CVE 生成攻击图

前面说到的系统存在着两种输入，一个是数据包，另一个就是判定数据传输产生异常的条件了。

因为我们获取到的数据包当中只有时间、IP地址、端口、数据长度等几种信息，所有我们想要判定是否存在漏洞，一般智能从以下两方面来进行判定。

①根据流量的情况，如果单位时间内的流量传输较其他时间内的流量传输有巨大差别，此时也许主机之间的数据传输存在漏洞。

②CVE相当于是网络漏洞的字典，我们可以通过输入CVE当中的多种情况，然后分析数据是否存在漏洞。

4、显示攻击图过程

显示攻击图过程，这是系统着重实现的目标，为了让用户更好的使用我们的网络攻击图系统，我们必须直观的将攻击图显示出来。其中节点表示网络所处的状态，节点间的有向边表示网络状态间的转移关系。

这里初步的想法是使用Neo4j进行可视化。

2.1.2性能需求

1、支持5000以上结点

因为处理数据的大小是不确定的，以及漏洞存在的数量也是无法预计的，我们需要将系统优化，支持同时显示5000个以上的结点。

大量结点的显示可能会耗费大量的时间，系统设计过程当中如何优化系统，让其更快的分析数据，以及尽可能多的显示结点是系统的重要性能需求。

2、支持变速显示

因为我们发现读入的数据是按时间顺序排序的，当系统分析数据的时候，会逐渐显示结点的以及结点间的关系，我们应该在系统中添加控制组件，可以控制系统分析数据或者显示结点的速度。

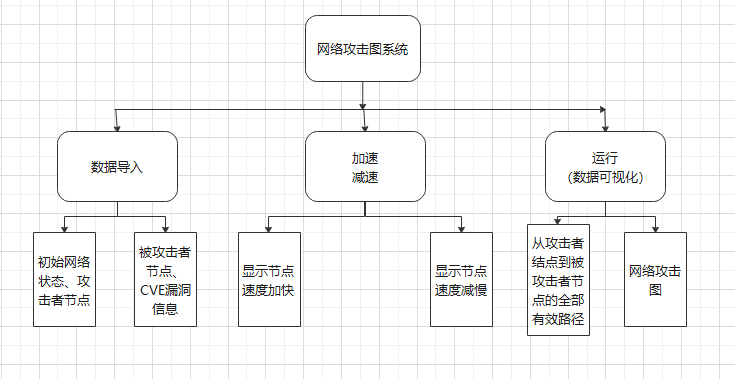
2.2运行环境

Windows 10 x64

处理器：INTEL 酷睿 I7-8550U 1.8GHz

内存：双通道8GB 2400MHz LPDDR4

2.3处理流程结构



2.4人工处理过程

需要人工导入数据，及窗口或菜单栏选项进行信息确认或者选择。

2.5尚未解决的问题

对变速显示功能需求的理解和实现思路

**3 接口设计**

3.1[用户接口](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7%E6%8E%A5%E5%8F%A3" \t "https://baike.baidu.com/item/%E6%A6%82%E8%A6%81%E8%AE%BE%E8%AE%A1%E8%AF%B4%E6%98%8E%E4%B9%A6/_blank)

用户采用窗口式或菜单栏设计

3.2外部接口

硬件接口

3.3内部接口

**4 运行设计**

4.1 运行模块组合

本系统主要以一个窗口为模块，有分别是导入数据、运行、生成可视化攻击图（加速减速）窗口，主窗口通过打开另一个子窗口来实现各个模块之间不同的功能连接和组合。个模块之间相对独立，程序的可移植性好。

4.2 运行控制

运行严格按照各个模块之间的函数调用关系来实现。

4. 3 运行时间

大量节点的显示可能会耗费大量的时间，系统设计要优化，更快的分析数据。

**5 系统数据结构设计**

网络攻击图由节点和连接节点的有向边组成。其中节点表示网络所处的状态，节点间的有向边表示网络状态间的转移关系。

模拟攻击者对存在安全漏洞的网络攻击过程，找到所有能够到达目标的攻击路径，同时将这些路径以图的形式表现。

漏洞信息

　 attackRule(connProto, vuls)

connProto 攻击者和被攻击者所应当满足的协议

vuls 攻击所依赖的弱点，依据CVE协议

算法思路：

1、广度优先算法

2、正向搜索或正向与逆向搜索同时进行（基于给出的防火墙等关键节点）

**6 系统出错处理设计**

6. 1 出错信息

加速节点显示导致系统停止运行。

6. 2 补救措施

尽量显小数据规模，减小同一时间内读入内存的数据。

6. 3系统维护设计

我们采用模块化的设计方法，每一个模块（窗口）之间相互独立性较高，这样方便进行软件维护，对于单独功能的修改只需要修改单独的窗口就行，对于功能的添加，只需要添加菜单项的内容即可。