**《概要设计文档》**

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **修订描述** | **修订者** |
| 2020.9.8 | v1.0 | 初稿 | 柯杭、邱瑞亨 |
|  |  |  |  |
|  |  |  |  |

目 录

[1.引言 1](#_Toc50498111)

[1.1编写目的 1](#_Toc50498112)

[1. 2项目背景 2](#_Toc50498113)

[2.总体设计方案 2](#_Toc50498114)

[2.1设计前提和约束方案 2](#_Toc50498115)

[2. 2系统整体设计 2](#_Toc50498116)

[2. 3性能要求 2](#_Toc50498117)

[2.4运行环境 2](#_Toc50498118)

[2. 5软件需要的人工处理过程 2](#_Toc50498119)

[2. 6概要设计尚未解决的问题 3](#_Toc50498120)

[3 接口设计 3](#_Toc50498121)

# 1.引言

## 1.1编写目的

本概要设计本党主要用来指导网络被攻击过程图形化显示系统的详细设计工作，为设计提供详细统一的参照标准。同时，此文档还作为审计依照的标准之一。

在详细设计的过程中，如果发现了需要添加的新的标准，则需要在项目管理工具中更新此文档并且重新进行评审，保证哥哥模块的详细设计一致性和正确性。

## 1.2项目背景

随着网络的普及大众化，越来越多的普通人投身于网络世界中，但是随之而来的是大量不法分子为了投机取巧，利用大众网络安全还未完全普及的情况，不断通过大量流量的涌入，攻击各个网络用户，以谋求巨额的利益。

为了直观了解到在某一时刻某片区域的网络攻击与被攻击的状况。我们决定研发出此系统。

此系统的功能：通过从本地导入网络相关文件，通过数据的分析和提取，找到某一时间点正在实施的攻击行为，将攻击的动作图形化，方便用户的 观察和分析。

# 2.总体设计方案

## 2.1设计前提和约束方案

①使用python语言的使用规范

1. 输入数据集仅限csv数据集

## 2.2系统整体设计

通过读取文件中的数据，经过一定的处理后可视化。

采用固定时段的网络状态，分析出攻击行为，并且以箭头的形式显示出来，攻击的规模越大，箭头越粗。同时不同的协议也有着不同的颜色。

用户通过选择时间速度和时间进度来观察特定时间段的流量变化和被攻击

状况。

## 2.3性能要求

支持5000个节点的网络被攻击图显示；支持对时间变化变速浏览被攻击图状况。

## 2.4运行环境

Python3.8于Windows10环境下

## 2.5软件需要的人工处理过程

选择含有时间、协议、目的地址、源地址、长度的csv数据集文件作为输入；拖动时间条选择速度以显示节点被攻击情况。

# 3.接口设计

|  |  |  |  |
| --- | --- | --- | --- |
| 功能模块 | 接口名称 | 输入 | 输出 |
| 导入导出 | 导入 | 网络文件 | 各类数据(源IP,目的IP,协议,时间,大小)，list |
| 导出 | 将系统中得到的某一状态导出 | CSV文件 |
| 数据处理 | 获得某时间段端口 | 时间段 | 获得某时间段端口（源IP,目的IP,协议,时间,大小） |
| 获取所有攻击端口 | 各类数据list | 攻击端口（） |
| 通过处理找到攻击记录 | 各类数据list | 攻击记录（源IP,目的IP,协议,时间,大小） |
| 数据可视化 | 将数据可视化 | 攻击记录（源IP,目的IP,协议,时间,大小） | 可视化图 |