需求说明书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **修改时间** | **修改人** | **是否审核** | **备注** |
| V1.0.0 | 2020/9/8 | 主文浩 | 是 |  |
| V1.1.0 | 2020/9/12 | 胡港 | 是 | 新增了一个功能需求和一个性能需求 |
|  |  |  |  |  |
|  |  |  |  |  |

# 一、编写目的

本需求说明书的编写目的是为了更加全面深入的了解项目的需求，为我们后期的项目进行、任务分配等多项工作奠定基础。只有进行全面的需求分析，才可以更好的理解项目，进行代码的编写以及项目实现。

# 二、项目概述

本次项目的目标是完成一个网络攻击图系统。

首先我们要了解什么是攻击图：网络中总是存在一定的安全漏洞，同时这些漏洞之间可能存在一定的关联关系，即当一个漏洞被成功利用后，可能为另一漏洞的利用创造有利条件。为了能够彻底找出所有关联关系，最有效的方法就是通过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，这种图就是网络攻击图，简称攻击图。与攻击树和Petri网相比，攻击图对网络攻击过程的描述能力更强，应用范围也更加广泛。

我们要做的就是根据老师给的Excel文件当中的数据，生成攻击图，我们的任务就是完成这样的一个攻击图系统。

# 三、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。

**5、建立弱点关联数据库**

弱点关联数据库为攻击图生成提供数据支持,生成体现攻击者权限提升过程的网络攻击图。系统的弱点关联数据库可以实现对弱点信息的数据挖掘,以表现攻击者权限提升的思想为依据,将弱点的使用前提和作用结果进行量化。

# 四、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。

1. **支持攻击图可视化**

许多现有的攻击图工具都采用一种特别的方式来表示输入信息和输出图的数据结构，这些工具一般需要专门设计的各种辅助输入的数据格式，而且由此生成的攻击图通常让人难以理解和使用，所以这些工具的使用价值较低。

我们可以通过一种聚合技术来控制攻击图的复杂度，从而实现攻击图可视化。