**告警攻击链挖掘算法1.0测试报告**

**完成人：徐子森**

**日期：2023-11-29**

# 算法概述及版本修订记录

|  |  |
| --- | --- |
| **摘 要** | 本测试报告为综合安全告警攻击链算法的测试总结报告。 |
| **算法简介** | 该算法主要用于在海量告警日志数据中快速挖掘潜在的链式告警行为，应用时序关联特征和告警间的拓扑连接关系，启发式搜索链式结构，辅助安全分析人员快速了解网络安全态势与威胁风险。 |
| **当前版本代码来源** |  |
| **备注** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本修订记录** | | | | | |
| **编号** | **日期** | **版本** | **修 订 内 容** | **修订人** | **审核人** |
| 1 | 23/11/29 | v1.0 |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 算法输入输出

输入：告警ID，告警接收时间，源IP，源端口号，目的IP，目的端口号，告警类型，告警威胁等级

输出：告警攻击链

# 功能详述

综合安全告警攻击链算法主要包含如下功能点：

1. 利用网络告警日志数据启发式挖掘链式攻击结构
2. 实现链式攻击结构存储与分析
3. 用logging库记录算法测试结果用于分析

# 测试内容

本节介绍算法测试的方向与内容，包括但不限于以下几点

1）功能性：测试实现本算法的两种功能

2）稳定性：测试当有较大规模测试用例作为输入时算法依然能稳定运行

3）容错性：测试算法的异常处理能力

# 测试资源

## 研发人员

|  |  |
| --- | --- |
| **姓名** | **分工** |
| 徐子森 | 算法设计、算法测试 |

## 测试环境

|  |
| --- |
| **软件环境（编译环境、库版本等）** |
| Python3.7.6；  当前库版本： matplotlib==3.7.1  networkx==3.1  numpy==1.24.3  pandas==2.0.2  pymysql==1.0.2 |
| **硬件环境（网络、设备等）** |
| 无特殊要求 |

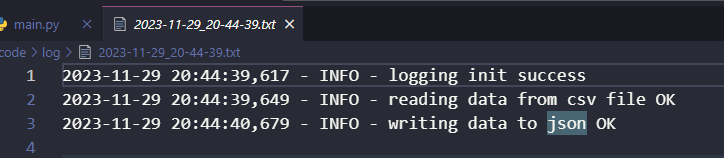
# 测试结果分析

## 测试用例及测试结果

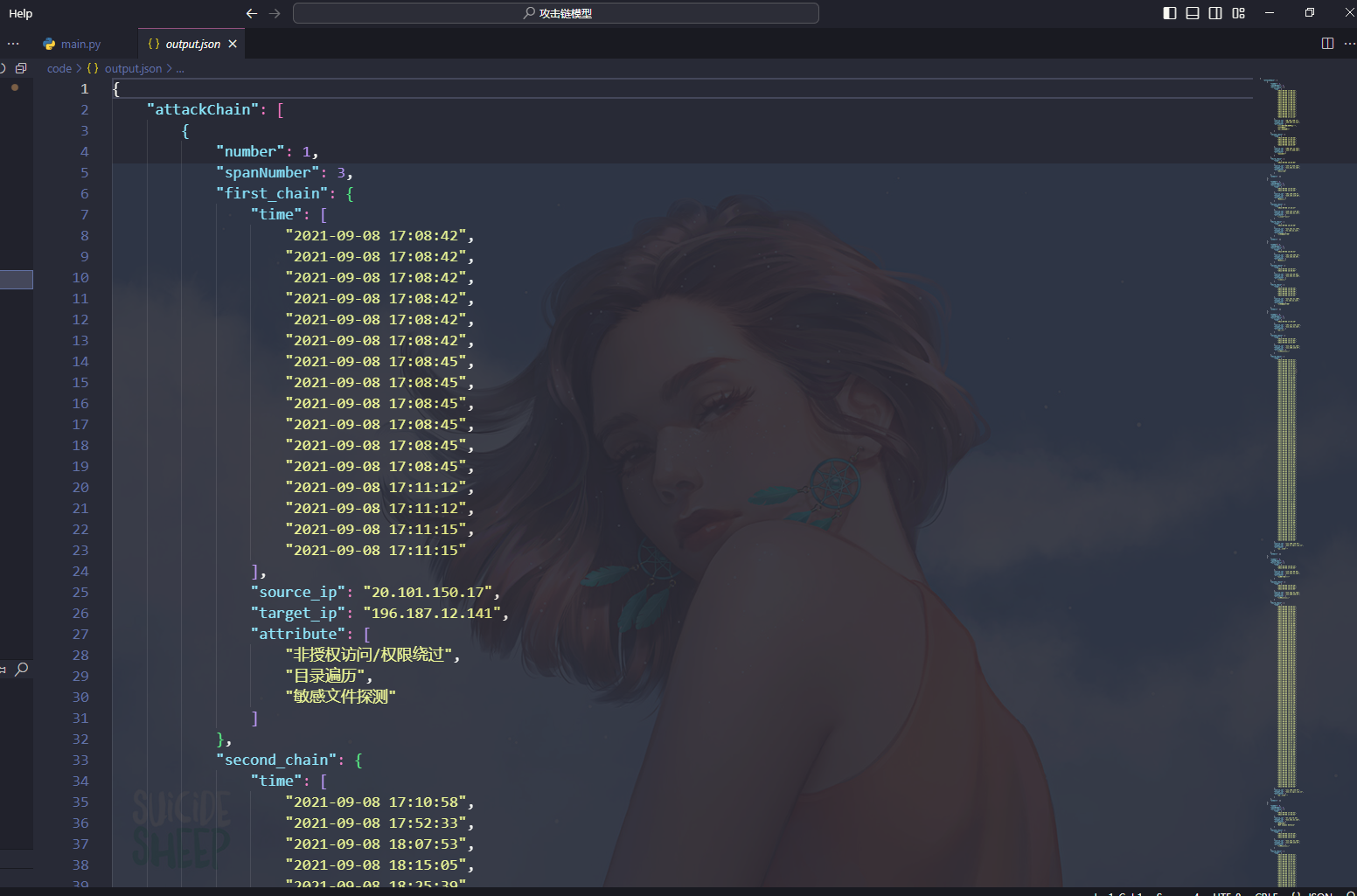
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **模块** | **功能点** | **测试用例** | **预期结果** | **测试结果** |
| 告警攻击链挖掘与存储 | 告警攻击链挖掘 | 测试输入数据集由14386条真实场景网络安全中采集的告警日志。算法读取整个告警日志数据集并启发式搜索链式攻击结构。 | 算法应输出长度超过4的链式攻击结构 | 通过 |
| 告警攻击链存储 | 通过 |

## 主要测试结果截图

**在样例数据中，从csv文件中读取告警数据以及将告警链挖掘结果写入json文件正常。**



**查看输出的json文件，格式正确。**



* 1. **测试结果分析**

从上述测试内容来分析测试结果

1. 功能性：能够实现基于csv表格数据读取的网络告警攻击链挖掘与分析功能。但后续和采集数据库对接时需改写数据读取接口的代码。
2. 稳定性：能支持将近一万五千条数据规模的测试用例的快速的结果输出，运算时间只需2秒。
3. 容错性：

当测试用例中出现缺失值或表格数据读取失败时算法会跳出异常。不过目前本算法仅支持这两种异常，当其他异常出现，或与采集数据库对接时可能需要增添其他的异常处理。

* 1. **算法性能等级评估**

分为五个等级：

E级（算法代码尚不完善，无法运行）

D级（算法代码已完成，但无法正常运行，功能需求未实现）

C级（算法代码能够正常运行，但部分功能不能被正确实现）

B级（功能实现基本能实现但还具有细微缺陷，如部分测试用例无法通过、稳定性不足等）

A级（功能全部完美实现）

|  |
| --- |
| **评估等级** |
| B |

# 下一步工作计划

基于现有算法版本与测试结果的下一步算法修订与研发计划

设计与采集数据库的对接接口，创建其他异常处理类。