# UDP以太网检测说明书

## 工程目的：

​ 对以太网UDP数据中的正常数据、端口扫描攻击数据、DDoS攻击数据进行三分类的决策树模型训练，以实现训练得到的模型对三类型的UDP数据（Normal、Scan、Flood）进行分类。

## 系统软件环境：

1. python3.8

2. python依赖包（numpy、pandas、seaborn、matplotlib、sklearn）

3. mosquitto-2.0.15-install-windows-x64.exe

4. mysql8.0

5. java 1.8.0\_351

## 操作手册：

### 1.以太网数据建模：

机器学习模型训练需要对采集到的以太网数据进行建模，采集到的.pcapng以太网数据文件使用CICFlowMeter软件进行特征提取，生成可以用来进行机器学习训练的数据，以下是使用流程：

1.打开目录 data\_process\_app\CICFlowMeter-4.0\bin下的CICFlowMeter.bat文件

2.点击Network，选择Offline模式

3.在Pcap dir中选择需要特征提取的.pcapng文件路径

4.在Output dir中选择特征提取后数据的存储路径

5.特征提取后的数据为.csv文件

图形用户界面, 应用程序

描述已自动生成

### 2.UDP的模型检测与智能识别

1.对提取特征后的.csv进行数据标注，正常数据标注'Normal'，端口扫描数据标注'Scan'，DDoS数据标注'Flood'

2.整合需要训练的数据集，生成文件UDP\_Process.csv

3.打开udp\_train.py,设置训练与测试属性：

​ a. train\_flag: 模型训练选择，0不训练，1训练

​ b.test\_flag:运行测试选择，0不测试，1测试

​ c.show\_cm:测试结果（混淆矩阵，精确率等）显示，0不显示，1显示

d.model\_file:模型存储文件地址

​ e.train\_file:训练文件存储地址

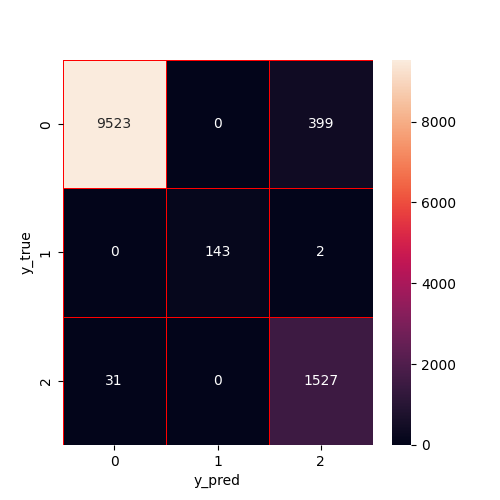
f.scaler\_file:标准化文件存储地址

g.encoder\_file:编码文件存储地址

4.运行udp\_train.py文件进行模型训练与检测

## 训练结果：

### 1.模型识别混淆矩阵



### 2.模型检测率

### 