23-24 夏季学期<<网络空间测绘与安全应用>>

云 IP 归属测绘作业要求

一、背景

基于云环境部署的服务往往缺乏备案信息，增加网络环境的不透明度，导致监管难度和安全防护难度的大幅提升。掌握云端托管服务所有者信息对于防范网络攻击、追踪失控资产、发现违规跨境传输行为等至关重要。

本次作业面向云托管的服务归属，通过融合被动流量行为信息和主动节点探测信息推断云上 IP 承载服务的所属者。

二、作业描述

2.1 主动探测

对云服务厂商（包括但不限于阿里云、腾讯云、华为云、亚马逊云）其拥有的 IP 做归属测绘分析，即判断某 IP 承载的服务归属，**如 163.181.199.199 属于阿里（归属到机构名称或个人）。**服务包括但不限于 web 服务、文件传输服务、邮件传输服务、数据库服务、基础设施服务。

2.2 被动分析

根据给定的信工所办公区被动流量日志，判断流量中哪些云 IP 属于信工所，可结合主动探测信息做交叉验证。

被动流量日志地址：

https://pan.baidu.com/s/1h2X7ny_CMA-J4J8FQWOrOQ?pwd=6wa9

2.3 开放思考

如果被动流量中存在多家单位流量，如何准确地将各单位与其拥有的云 IP 对应起来，请在实验报告中给出方案设计。

三、参考实现步骤

3.1 主动探测方法参考

1. 获取云的 IP 地址范围；
2. 探测云 IP 上开着哪些服务；
3. 收集信息，推断服务的所有者；
    - 域名，证书等信息
    - 网站备案信息
    - 图标信息
    - 文本介绍信息

3.2 被动分析方法参考

方法一：

1. 确定种子 IP，即一定属于信工所的客户端 IP；
2. 通过种子 IP 扩线，记录客户端 IP 访问的其他 Server IP；
3. 从 Server IP 中剔除流行服务，计算 Server IP 交集；
4. 通过主动方法做验证。

方法二：

1. 确定种子 IP，即一定属于信工所的云 IP；
2. 通过种子 IP 扩线，观察客户端访问该 IP 时，时间窗口 Ts 内还访问了哪些 IP；
3. 通过主动方法做验证。

四、作业提交

1. 汇报时间：**7 月 5 日**完成云 IP 归属测绘作业 PPT，展示小组对作业背景，方法的理解，随堂汇报，**汇报时间控制在 8 分钟以内**。

2. 作业提交时间：**7 月 14 日 23:59** 前提交作业到助教邮箱 zhangziwei@iie.ac.cn，包括云 IP 归属测绘作业全部内容以及一份组内成员分工介绍表。

3. 作业提交内容：

- **主动探测与被动分析分别形成 IP 归属列表（共两份），包含云 IP 与其对应的组织/个人归属（excel 或 json 文件）。主动探测要求归属 IP 数量不少于 1000，被动分析部分 IP 数量不作要求。**
- 作业全部过程形成实验报告，要求逻辑清晰，内容详实。包含背景、方法、创新点、开放思考、总结与收获。**鼓励同学们不拘泥于参考方法，将根据创新性额外加分。**
- 实验全部代码。

4. 作业提交形式：PPT+两份 IP 归属列表+实验报告+实验代码+分工介绍表，全部打包为一个压缩文件，命名为：第 X 组+所有小组成员姓名+学号。如，第一组+张三 202318011840033+李四 202318011460032+…

附录

被动流量日志说明

日志共包含三份文件,DNS_COLLECT_LOG、HTTP_COLLECT_LOG、SSL_COLLECT_LOG,内容为信工所办公区 6 天时间内的 DNS、HTTP 与 SSL 流量日志。

日志字段说明

DNS_COLLECT_LOG
RECV_TIME：日志进库时间
START_TIME：流开始时间
END_TIME：流结束时间
PROTOCOL：协议
CLIENT_IP：客户端 IP
CLIENT_PORT：客户端端口
SERVER_IP：服务端 IP
SERVER_PORT：服务端端口
NEST_ADDR_LIST：客户端 IP 与 DNS 服务器对应
DNS_QNAME：DNS QNAME

HTTP_COLLECT_LOG
RECV_TIME：日志进库时间
START_TIME：流开始时间
END_TIME：流结束时间
PROTOCOL：协议
CLIENT_IP：客户端 IP
CLIENT_PORT：客户端端口
SERVER_IP：服务端 IP
SERVER_PORT：服务端端口
HTTP_URL：HTTP 请求 URL
HTTP_HOST,：HTTP HOST 字段
HTTP_METHOD：HTTP 请求方法
HTTP_RETURN_CODE：HTTP 响应码
HTTP_USER_AGENT：HTTP UA 字段
HTTP_COOKIE：HTTP COOKIE 值
HTTP_REQUEST_LINE：HTTP 请求行
HTTP_RESPONSE_LINE：HTTP 响应行
HTTP_REQUEST_CONTENT_TYPE：HTTP 请求 CONTENT_TYPE 字段
HTTP_RESPONSE_CONTENT_TYPE：HTTP 响应 CONTENT_TYPE 字段

SSL_COLLECT_LOG
RECV_TIME：日志进库时间
START_TIME：流开始时间
END_TIME：流结束时间
PROTOCOL：协议
CLIENT_IP：客户端 IP
CLIENT_PORT：客户端端口
SERVER_IP：服务端 IP
SERVER_PORT：服务端端口
SSL_SNI：SNI 字段