01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

1. **作业内容**

作业布置

1、理解域名和子域名

2、学会如何收集网站、APP、小程序资产3、收集腾讯、字节、阿里、百度、拼多多 资产(任选其一)

1. **操作步骤**
2. 域名（Domain Name）：互联网上用于标识网站的名称，如 baidu.com；
3. 子域名（Subdomain）：在主域名之前添加前缀形成的地址，如 pan.baidu.com 是 baidu.com 的子域名；
4. 作用：子域名常用于区分不同服务模块，如邮箱、文件服务、用户系统等。
5. 在fofa查找





1. 在企查查搜索百度  
   
2. 在ICP/IP地址/域名信息备案管理系统查找“百度在线网络技术（北京）有限公司”





1. **作业总结**

1.初步掌握了域名与子域名的概念与实际用途

通过本次作业，我深入理解了“域名”与“子域名”的区别与联系。域名是互联网资产的入口标识，而子域名则通常代表企业旗下不同业务系统或模块。以百度为例，其主域名为 baidu.com，而 pan.baidu.com 则为网盘系统，tieba.baidu.com 是贴吧服务，这种结构清晰划分了各项业务，也为后续的资产识别与漏洞分析提供基础依据。

2.掌握了基础的资产收集方法与常用工具的使用方式

我借助 FOFA、企查查、工信部备案系统等公开信息平台，对百度公司的互联网资产进行了结构化收集。通过 FOFA，获取了数百个与百度相关的子域名、开放端口与指纹技术信息；在企查查中，查阅了其工商注册信息与对外控股关系；备案系统则确认了主办单位和域名的归属。这些平台的结合使用使我理解了信息收集应从“横向全面”与“纵向验证”两方面同步开展。

3.具备了从 APP 与小程序中提取网络资产的能力

除了传统网站资产外，我通过应用市场查询百度的移动端产品（如百度 APP、百度网盘等），并了解了如何通过 APK 包分析、抓包工具（如 HttpCanary、Charles）监测其通信域名和接口地址。小程序方面，通过微信内部搜索与抓包，识别了多个小程序后台请求的实际域名。这一过程让我初步具备了多平台资产识别的系统性意识。