**信息收集**

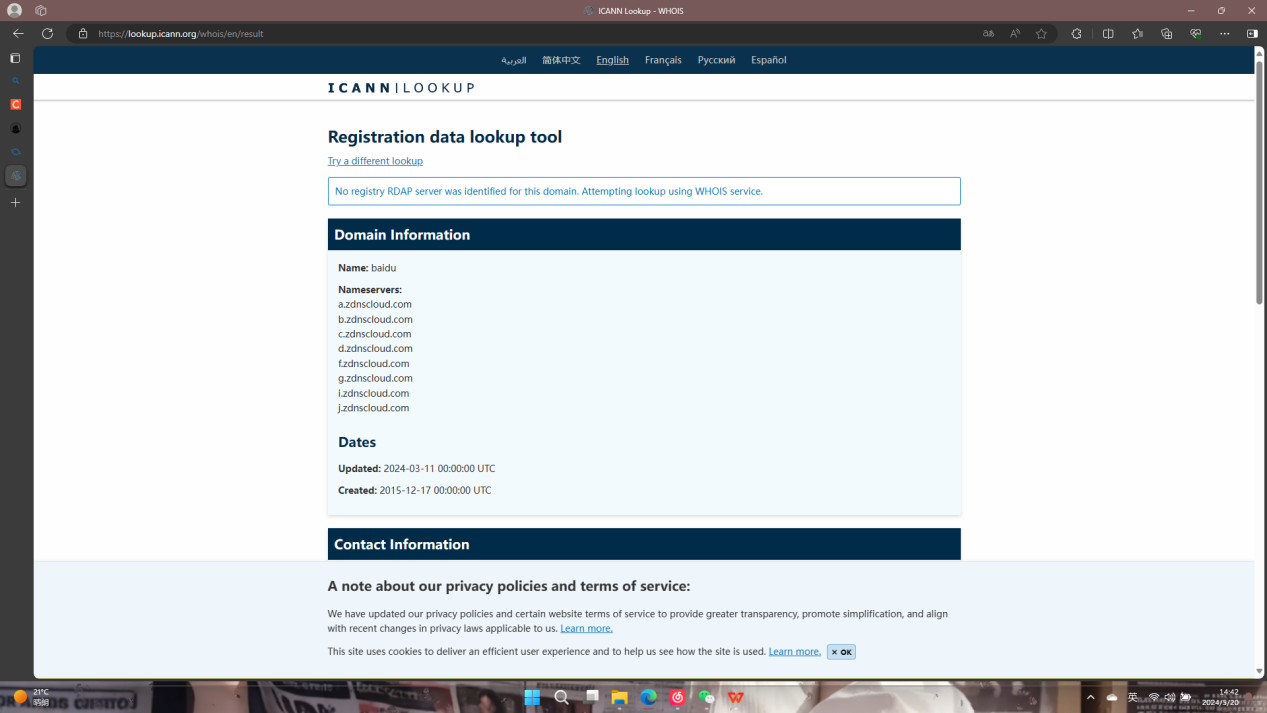
**1 公共网站全面IP、域名、注册等信息收集及分析：**

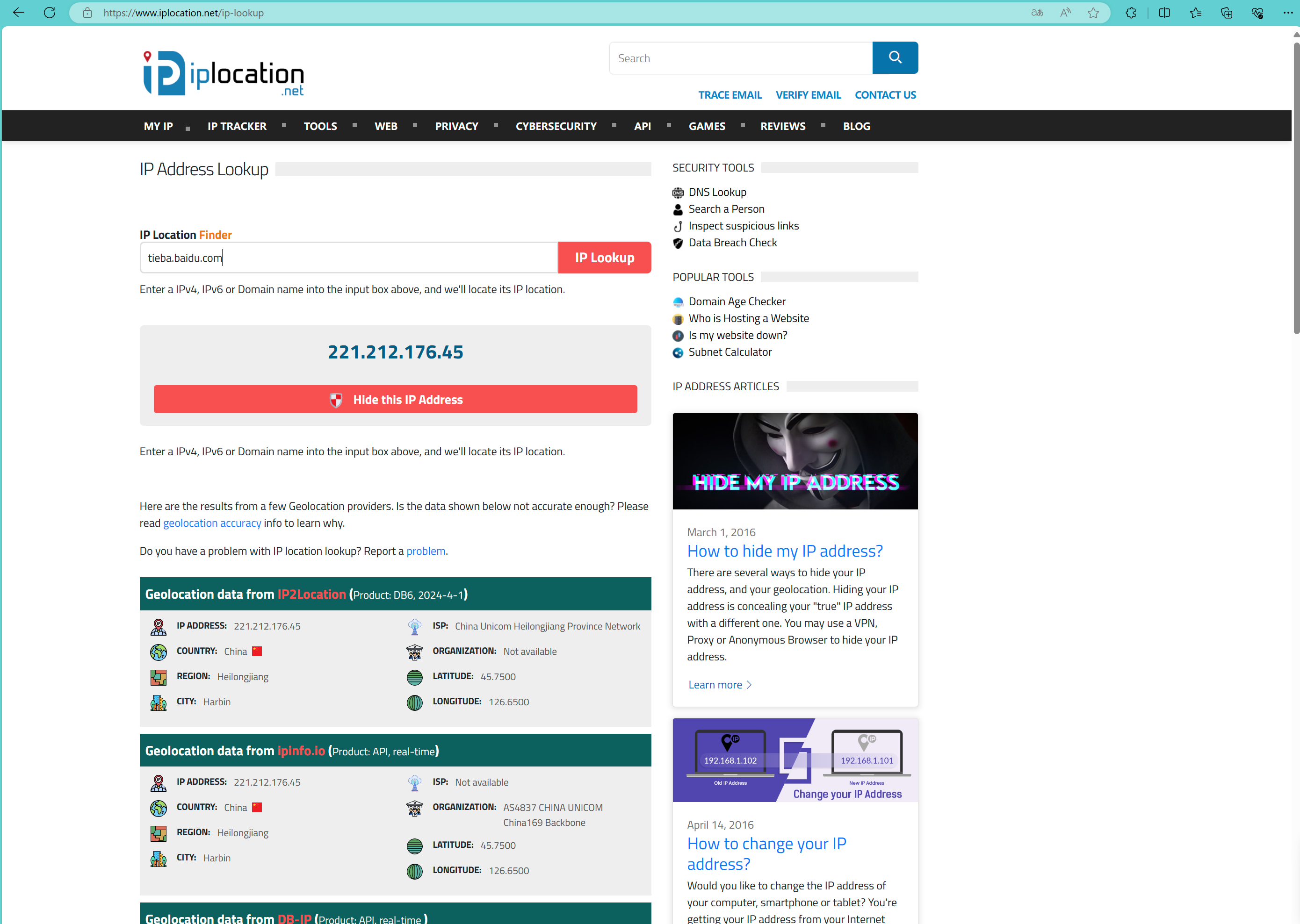
收集注册信息：

打开WHOIS查询网站，比如https://whois.icann.org/。

在查询框中输入baidu.com并点击查询按钮。

浏览返回的结果，查看域名的注册信息，包括注册者名称、注册日期、到期日期等。



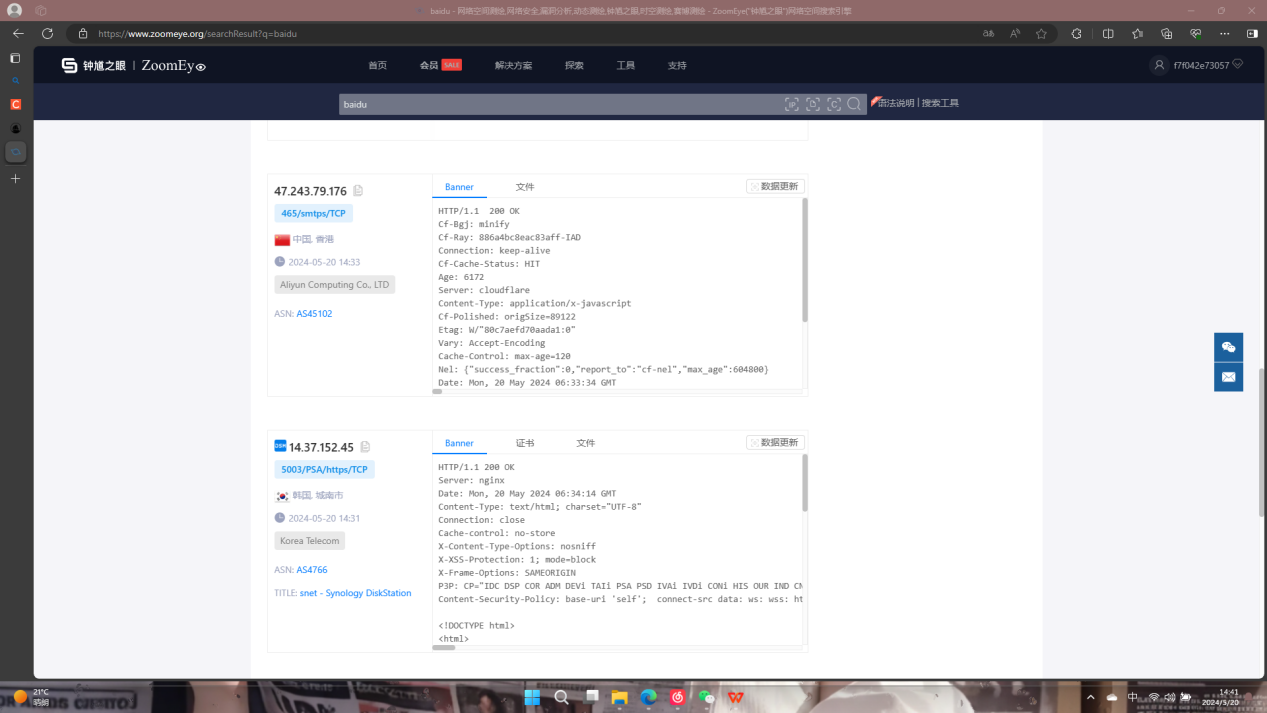


信息分析：

使用收集到的IP地址，可以通过在线IP定位服务（如https://www.iplocation.net/）来查找百度服务器的大致位置和网络提供商。

使用收集到的域名，可以进一步探索百度的子域名结构，例如tieba.baidu.com、wenku.baidu.com等，了解百度不同服务的域名组成。

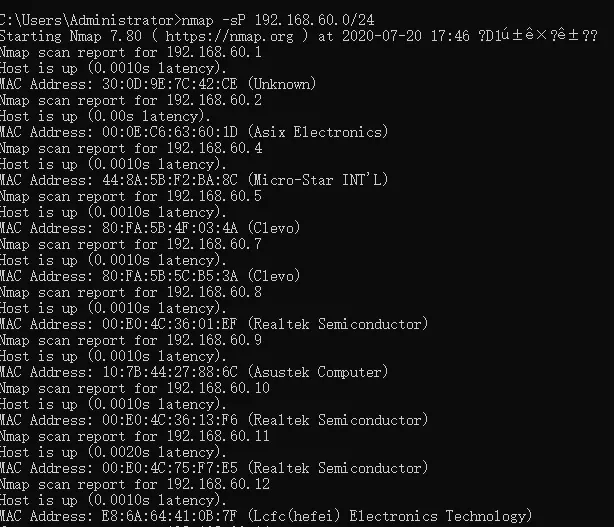
**2 使用互联网安全搜索引擎ZoomEye，和联网设备搜索引擎Shodan**

****

暴露的服务器、未经授权的访问、可疑的服务

**3 Nmap使用**

nmap批量扫描：



扫描IP地址范围: 可以指定一个IP地址范围

例：nmap -sP 192.168.60.20-100

漏洞发现参数

nmap脚本大概分类如下：

auth：负责处理鉴权证书（绕开鉴权）的脚本；

broadcast：在局域网内探查更多服务开启状况，如dhcp、dns、sqlserver等服务；

brute：提供暴力破解方式，针对常见的应用，如http、snmp等；

default：使用-sC或-A选项扫描时候默认的脚本，提供基本脚本扫描能力；

discovery：对网络进行更多的信息，如SMB枚举、SNMP查询等；

dos：用于进行拒绝服务攻击；

exploit：利用已知的漏洞入侵系统；

external：利用第三言的数据库或资源，例如进行whois解析；

fuzzer：模糊测试的脚本，发送异常的包到目标机，探测出潜在的漏洞；

intrusive：入侵性的脚本，此类脚本可能引发对方的IDS/IPS的记录或屏蔽；

malware：探测目标机是否感染了病毒、开启了后门等信息；

safe：此类与intrusive相反，属于安全性脚本；

version：负责增强服务与版本扫描（Version Detection）功能的脚本；

vuln：负责检查目录机是否有常见的漏洞（Vulnerability），如是否有MS08\_067；