2023 － 2024 学年 第 1 学期



### 实 验 报 告

课 程 名 C01218

课 程 号 网络安全防护技术

学 生 姓 名 张炳欣

学 生 姓 号 32201241

专 业 班 级 软件工程2204

所 在 学 院 计算机与计算科学学院 指 导 老 师 沈淳

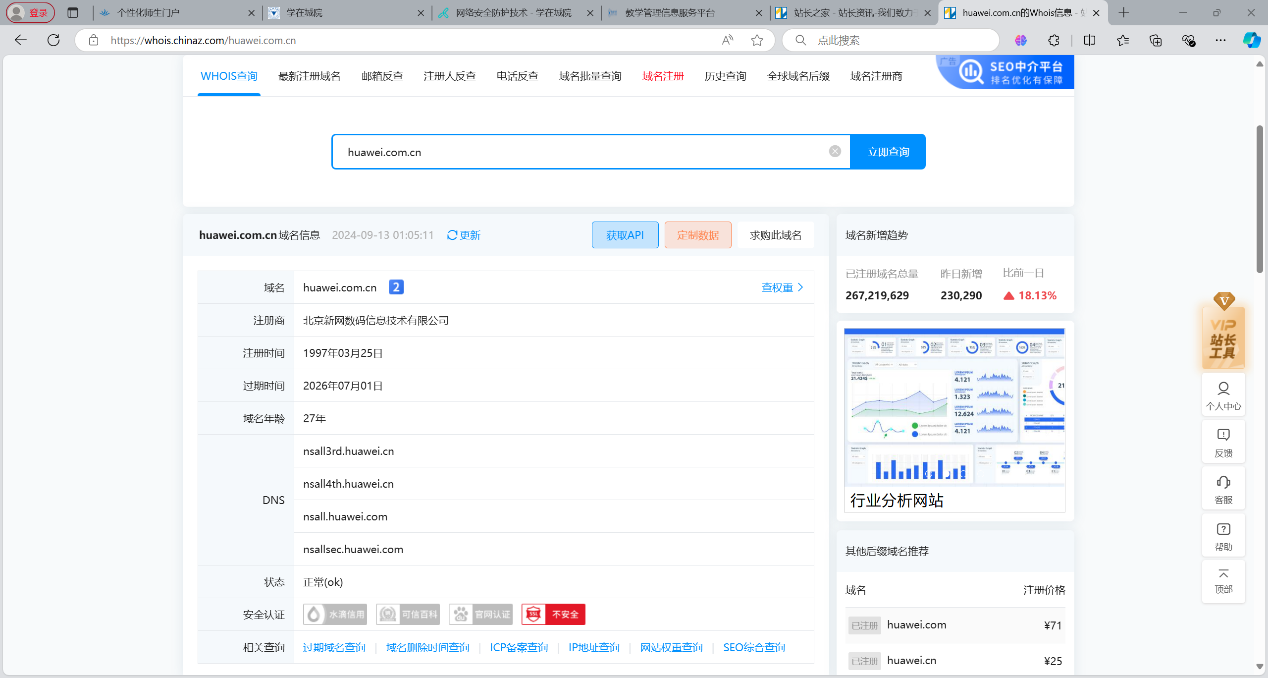
实验报告日期： 2024 年 9 月 19 日

**课程实验报告清单**

|  |
| --- |
| 目录 |
| 1.使用DNS whois查询huawei.com.cn的注册信息，再通过注册人信息对其进行whois反查。 |
| 2.使用IP whois查询浙江大学的IP地址详细信息。 |
| 3.使用工具查询202.10.195.195的具体地址在哪里（到城市）。 |
| 4.使用host和dig命令查询baidu.com域中的邮件服务器记录（提示：指定类型查询） |
| 5.分别利用dnsenum、dnsmap分别查找学校hzcu.edu.cn的子域名 |
| 6.用搜索引擎和JsFinder来分别查找baidu.com的子域名 |
| 7.使用netdiscover对本机进行ARP搜索 |
| 8.运行自己的phpstudy, nmap查看主机IP的开放端口号及对应的服务 |

完成要求：必须有详细过程。

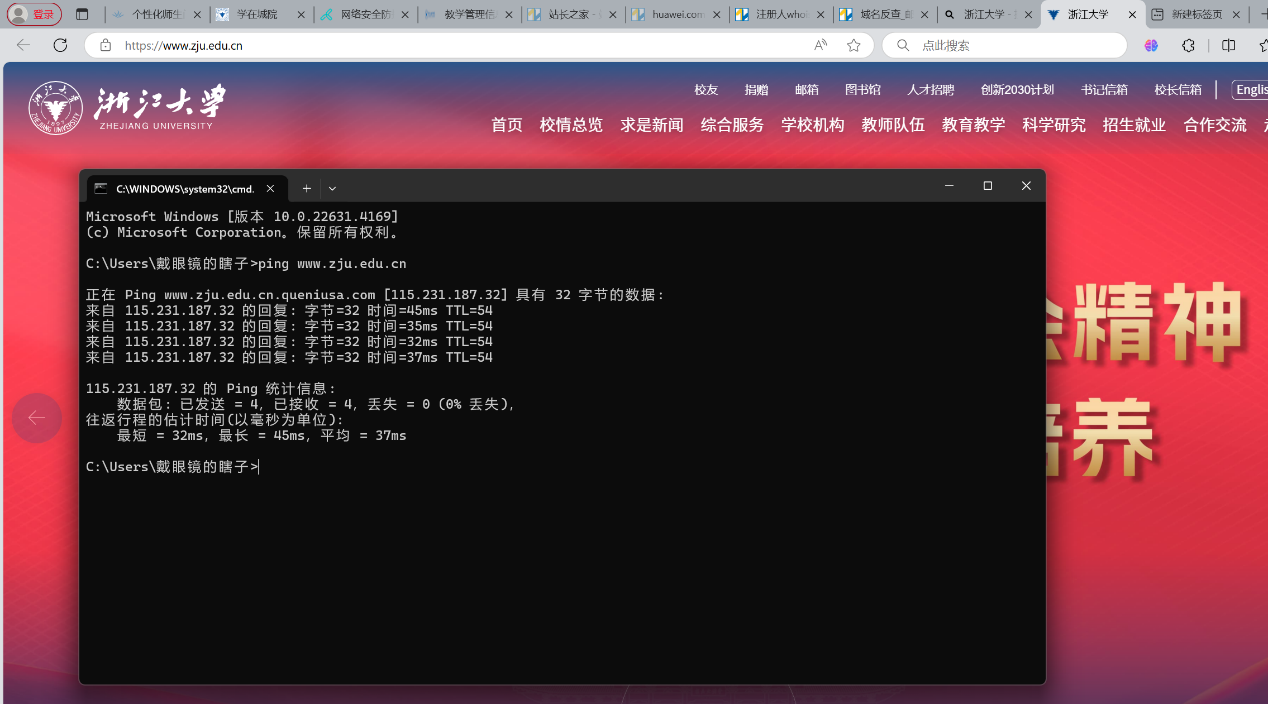
1. 使用DNS whois查询huawei.com.cn的注册信息，再通过注册人信息对其进行whois反查。



注册人反查

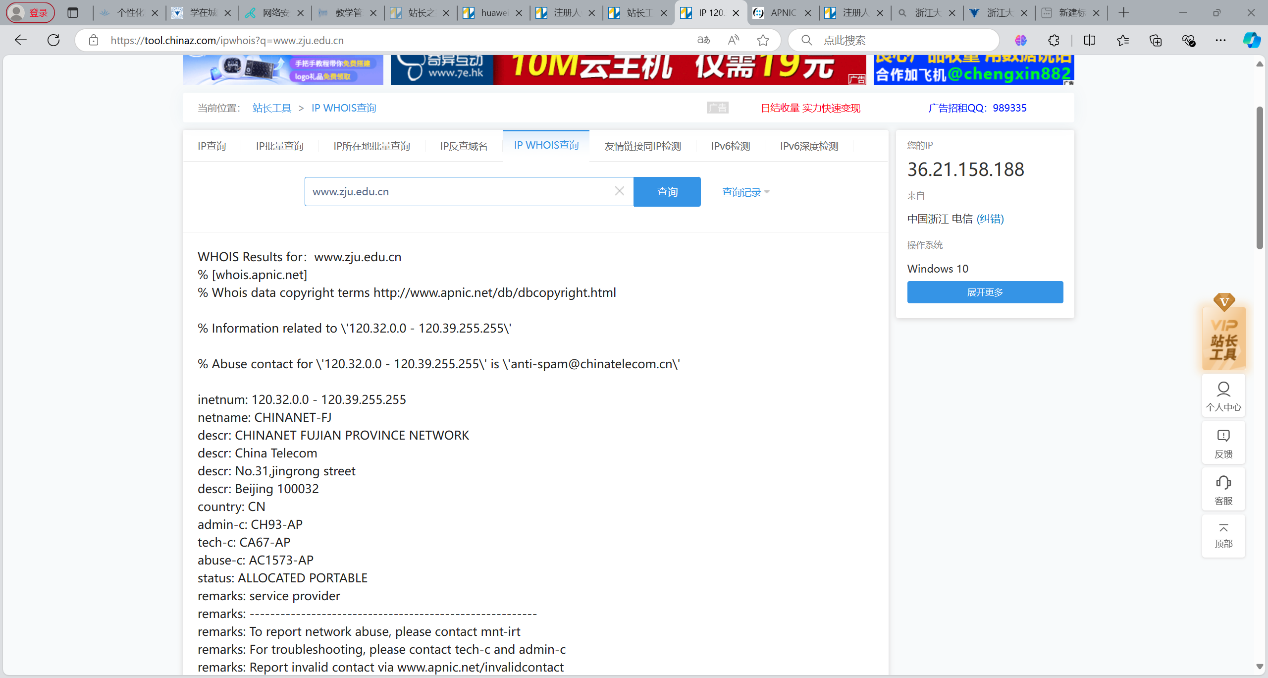


1. 使用IP whois查询浙江大学的IP地址详细信息。



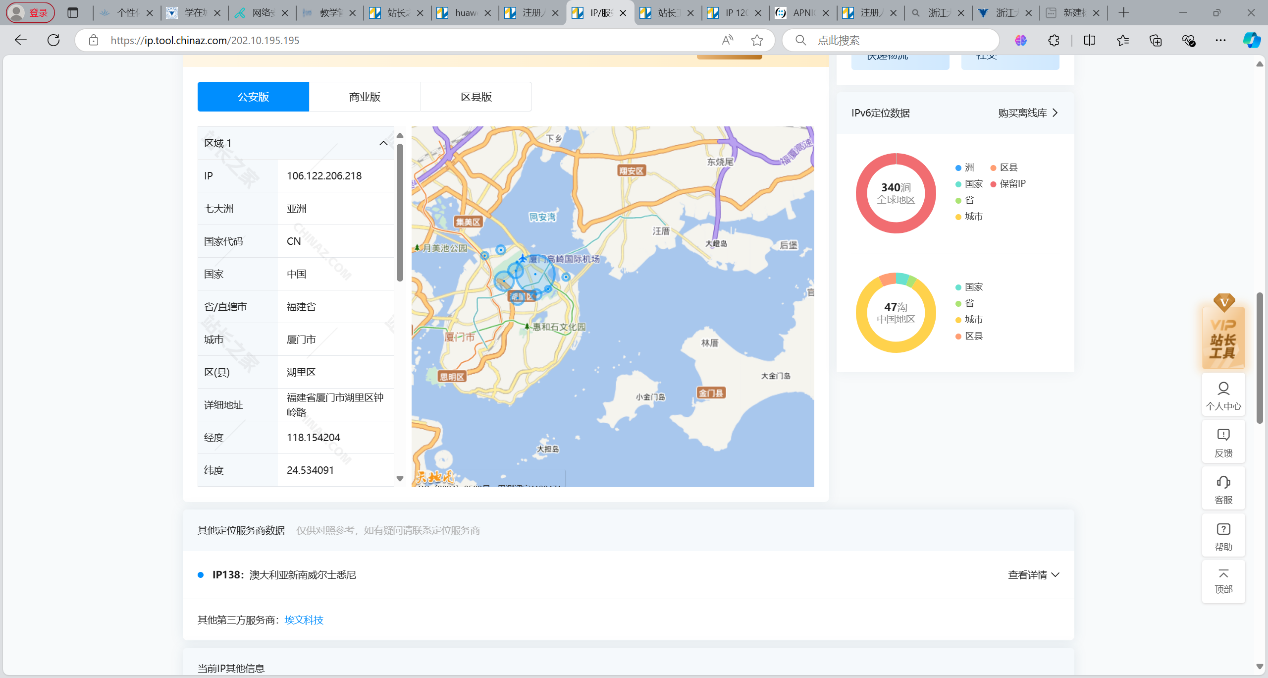
先通过浏览器找到浙大url 再pin找到ip

或者通过使用站长之家

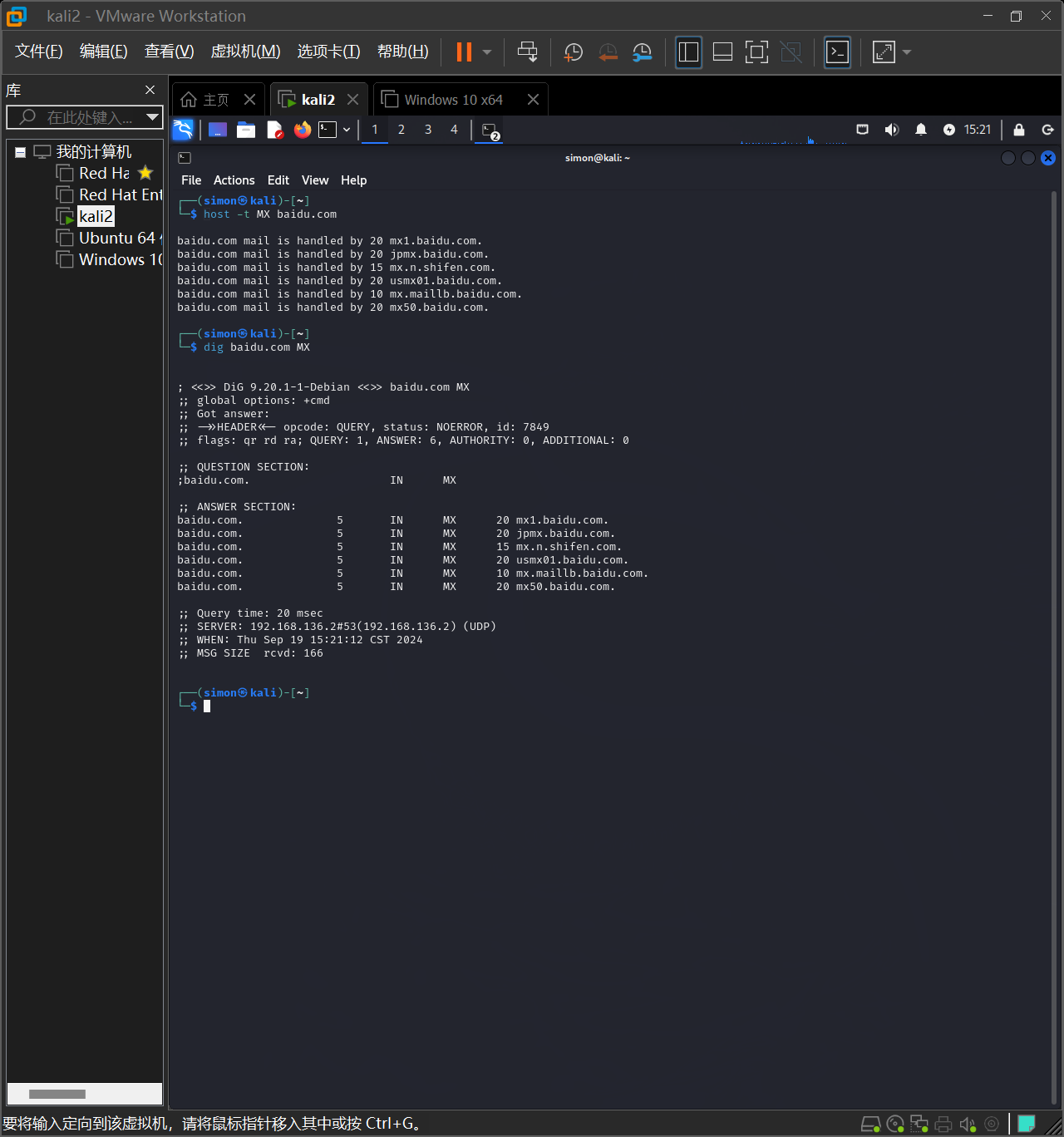


1. 使用工具查询202.10.195.195的具体地址在哪里（到城市）。

站长之家ip查询

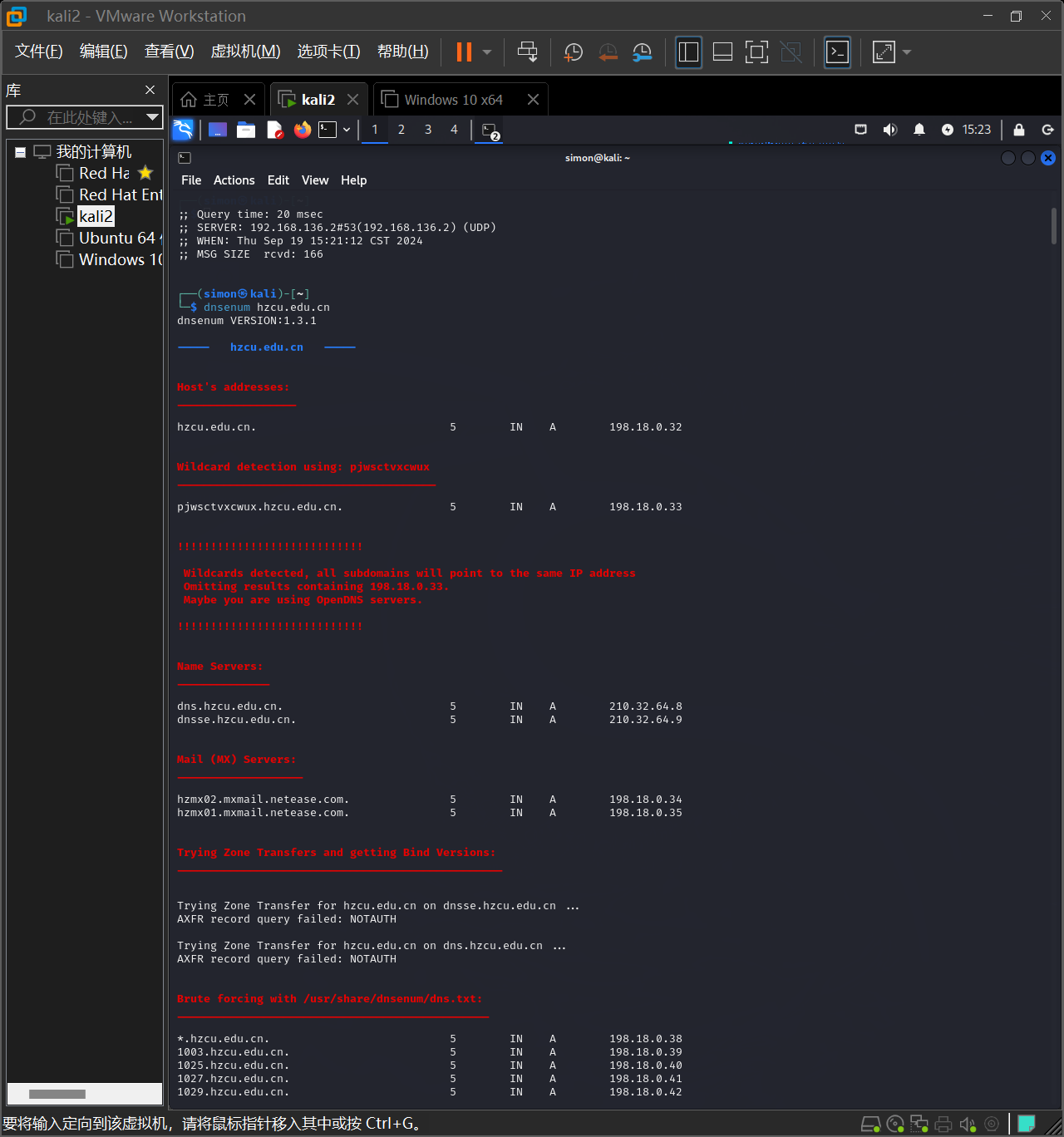


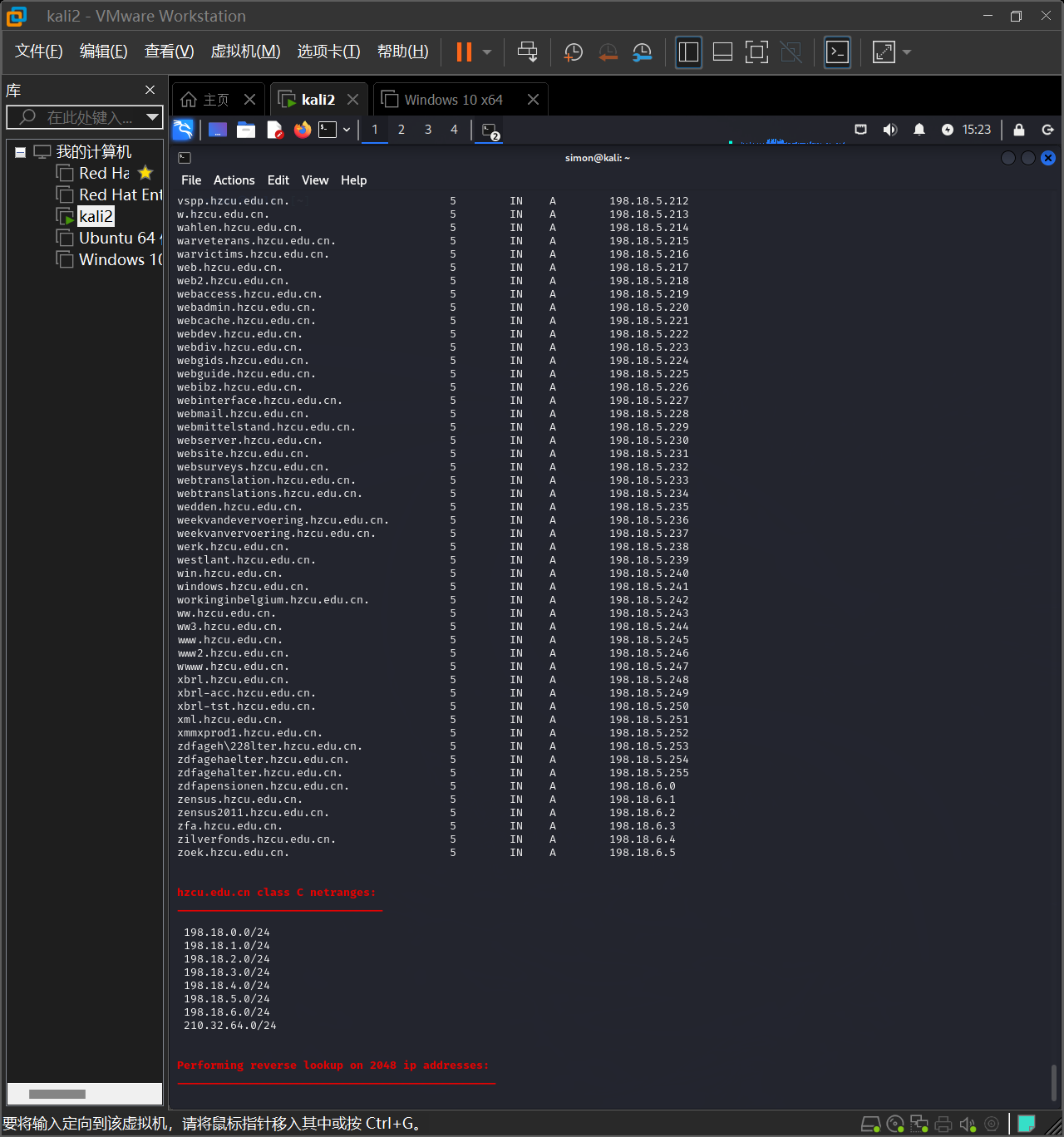
1. 使用host和dig命令查询baidu.com域中的邮件服务器记录（提示：指定类型查询）



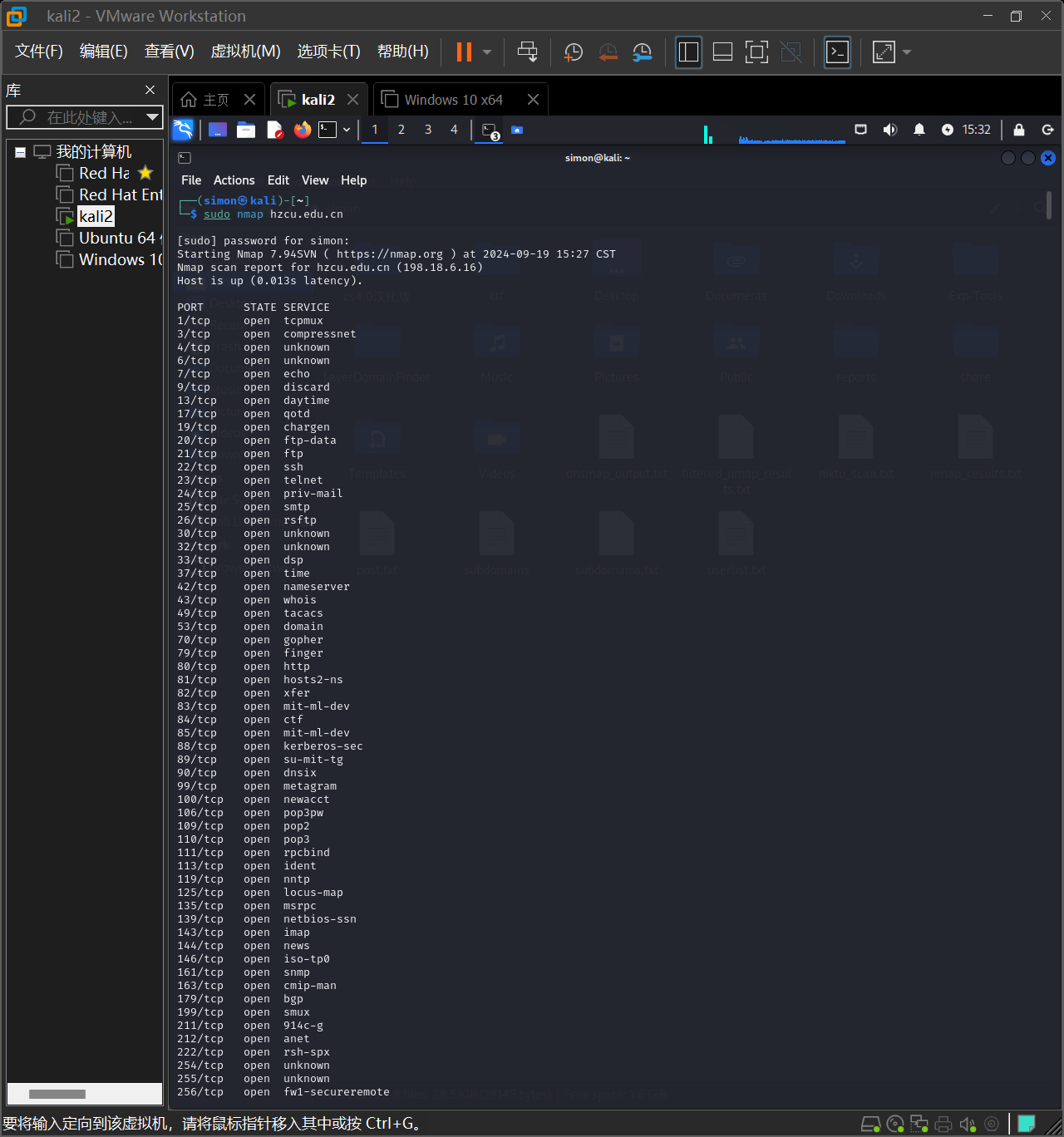
1. 分别利用dnsenum、dnsmap分别查找学校hzcu.edu.cn的子域名

Dnsenum：





Dnsmap：



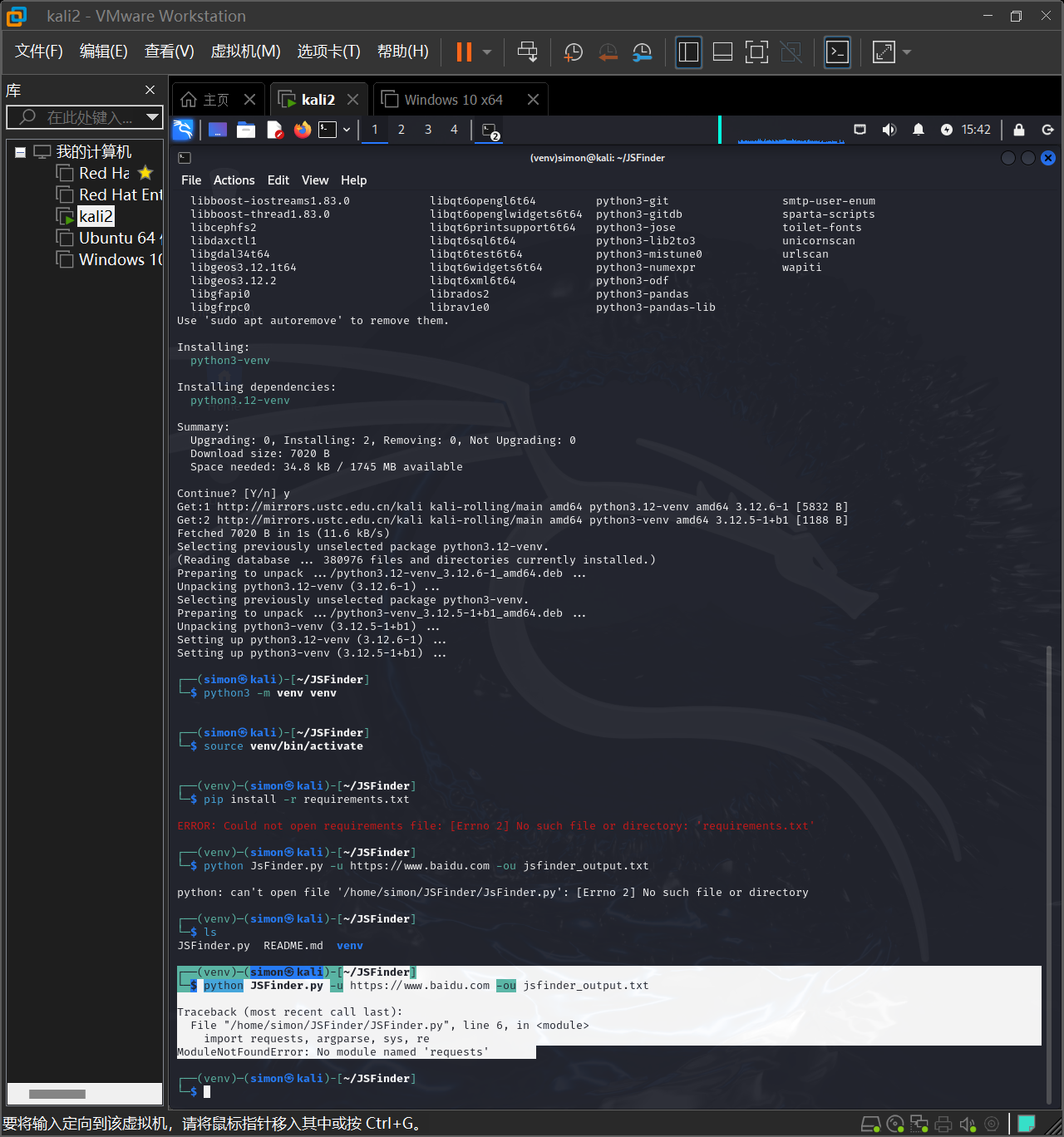
1. 用搜索引擎和JsFinder来分别查找baidu.com的子域名

搜索引擎（google）：

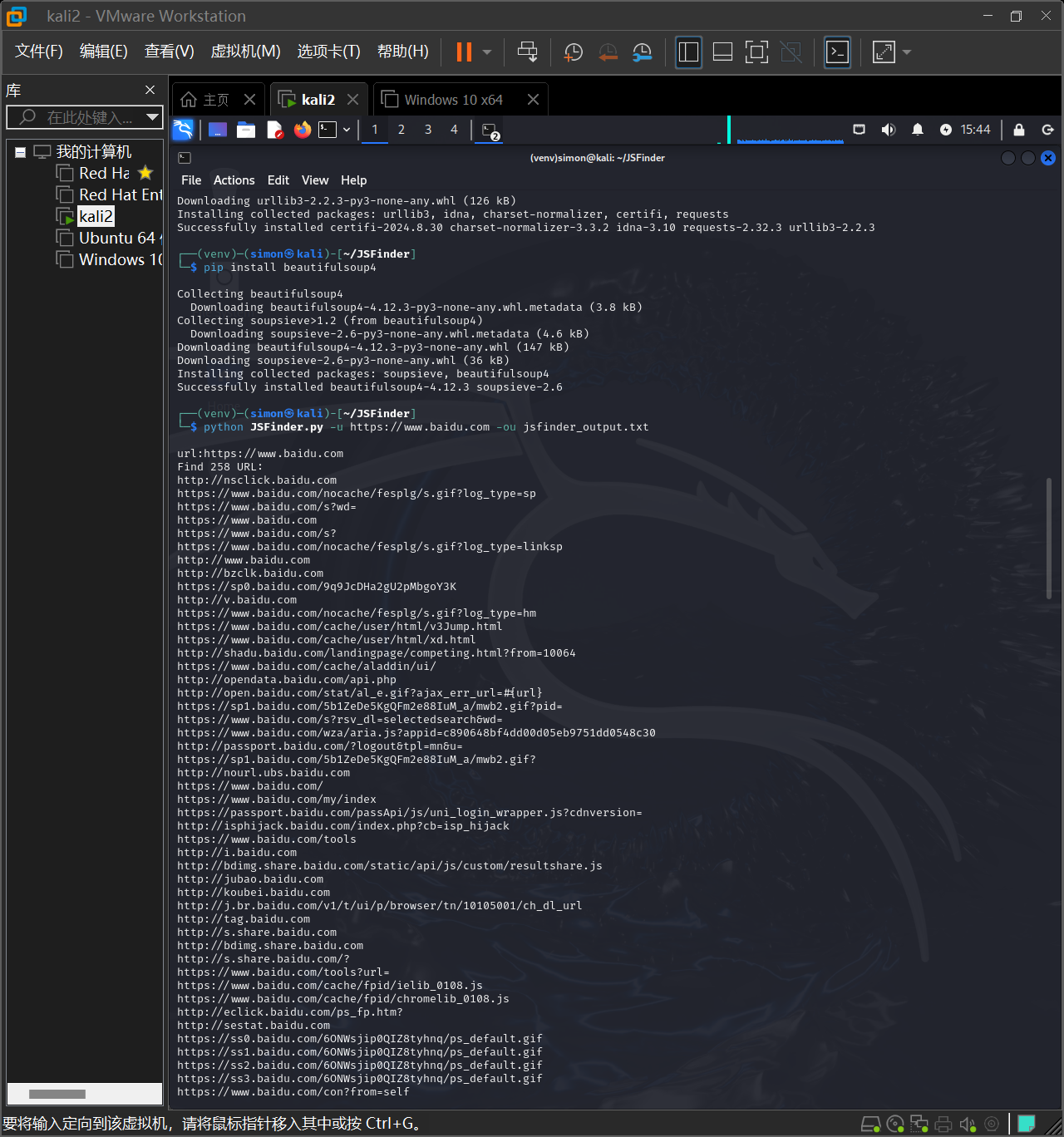


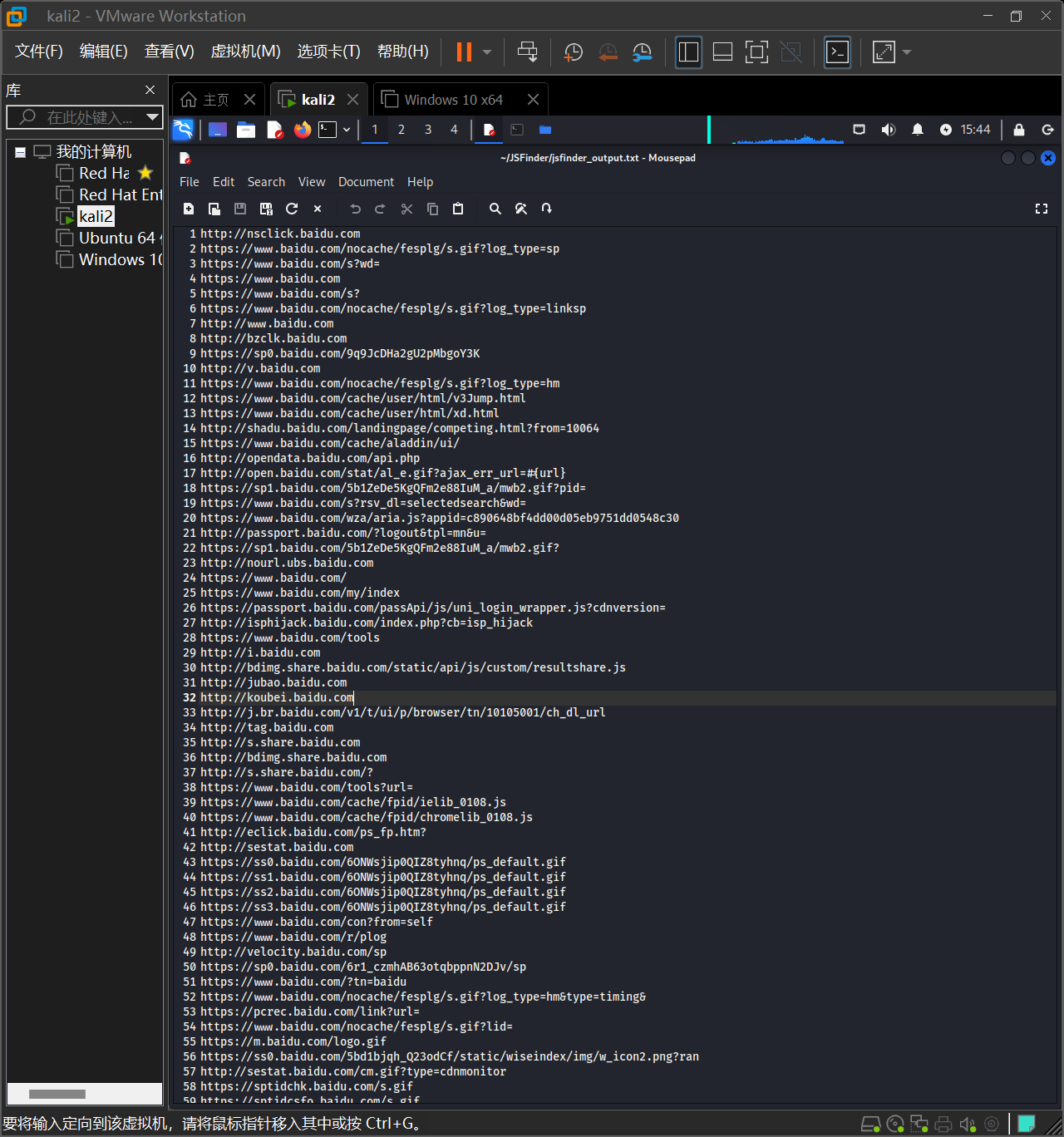
JF：

首先在kali里进行安装JF



安装好后直接py运行 结果输出到output文件里

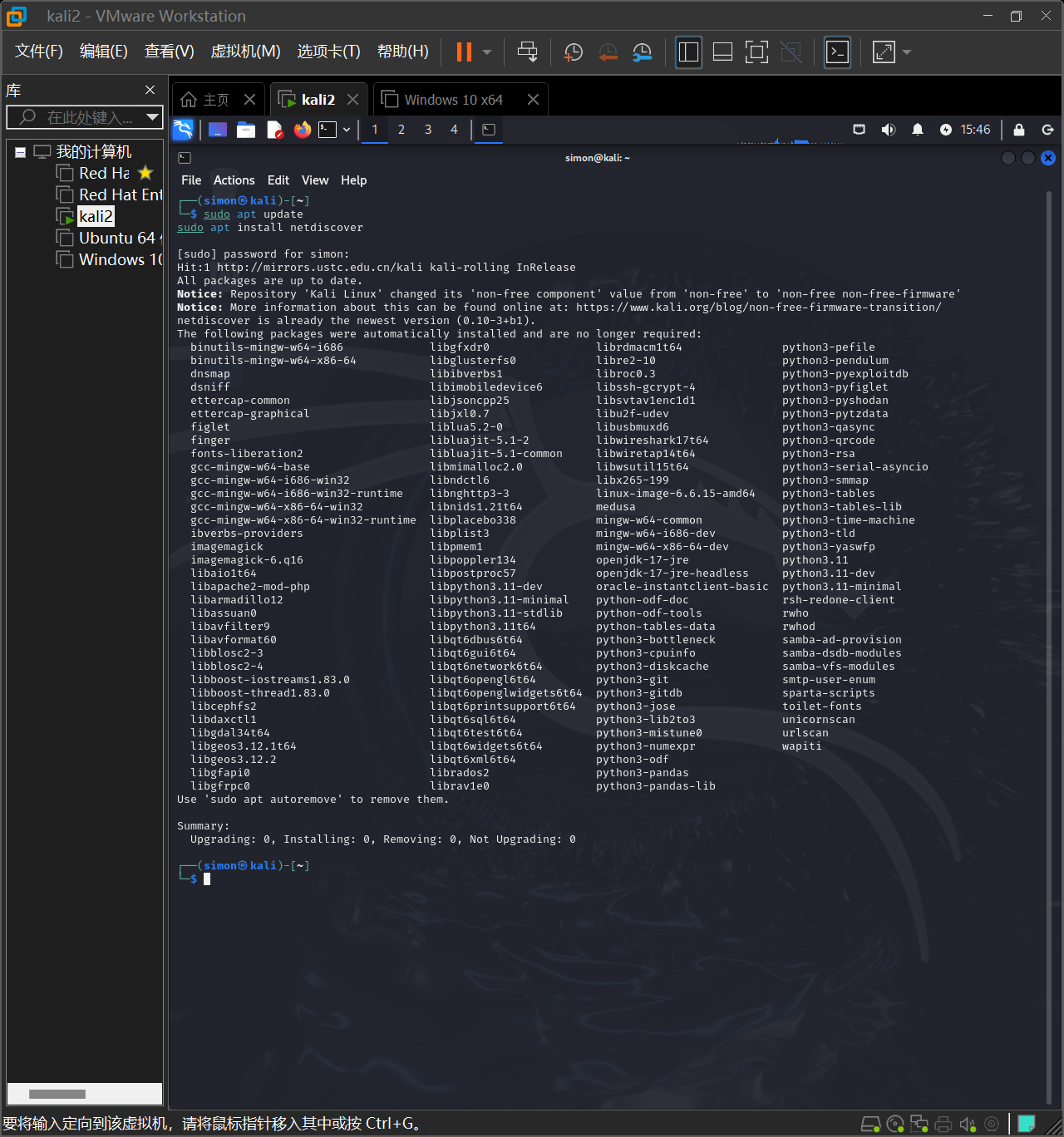


打开文件可以看到

1. 使用netdiscover对本机进行ARP搜索

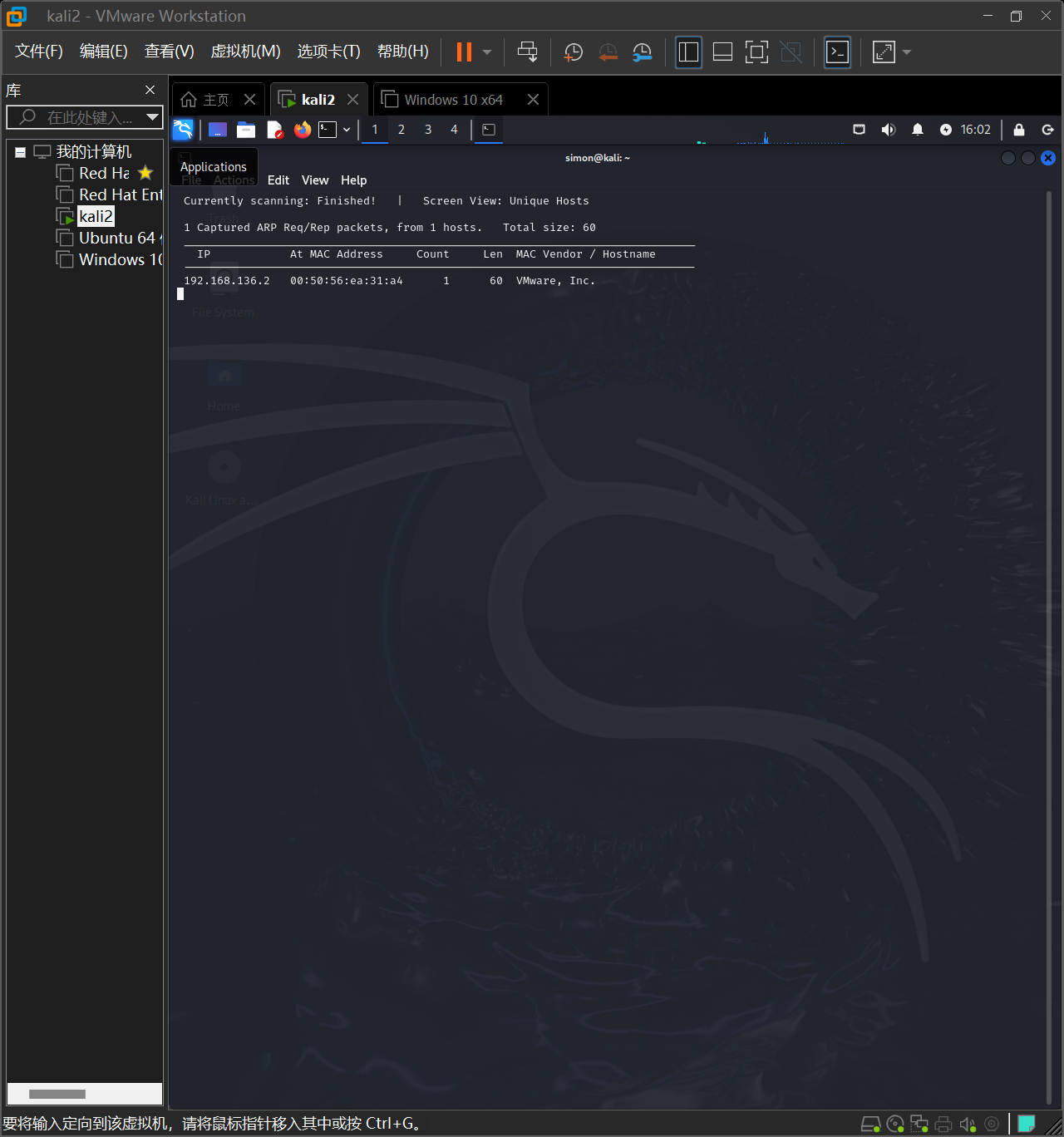
先进行下载

使用aptinstallnetdiscover



然后进行扫描 扫kali

sudo netdiscover -i eth0 -r 192.168.167.0/24



8.运行自己的phpstudy, nmap查看主机IP的开放端口号及对应的服务



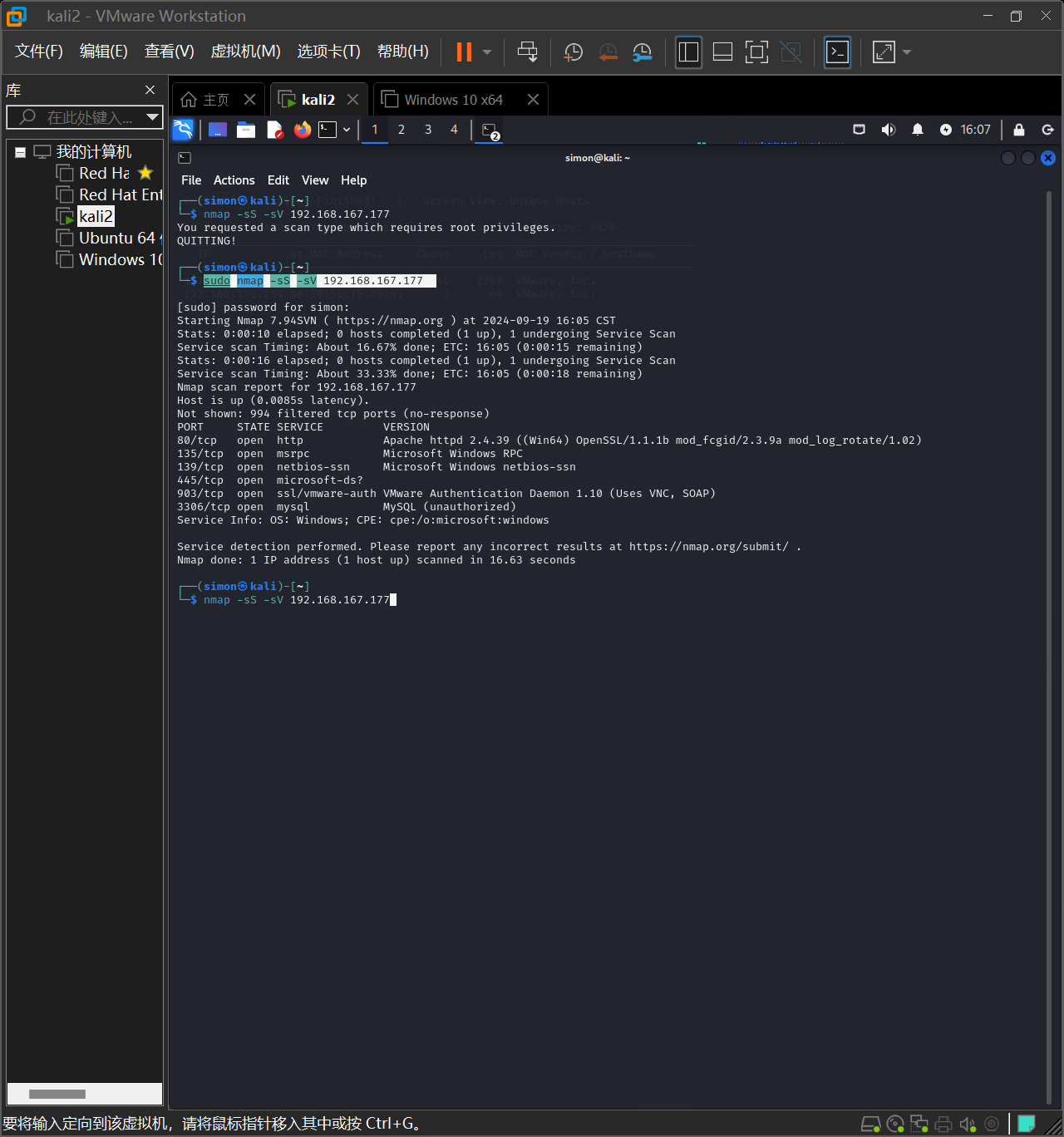
先启动phpstudy 把阿帕奇和mysql启动服务

阿帕奇端口是80 mysql是3306

然后进入kali 启动nmap

sudo nmap -sS -sV 192.168.167.177

ip为我自己电脑ip



结果出现

### 端口及服务说明

1. **80/tcp (HTTP)**:
   * **服务**: Apache HTTP Server 2.4.39
   * **备注**: 运行在 Windows 上，启用了 OpenSSL、mod\_fcgid 和其他模块。

2.**3306/tcp (MySQL)**:

* **服务**: MySQL 数据库
* **备注**: 显示为“unauthorized”，这表明 MySQL 服务没有启用授权或访问控制。