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

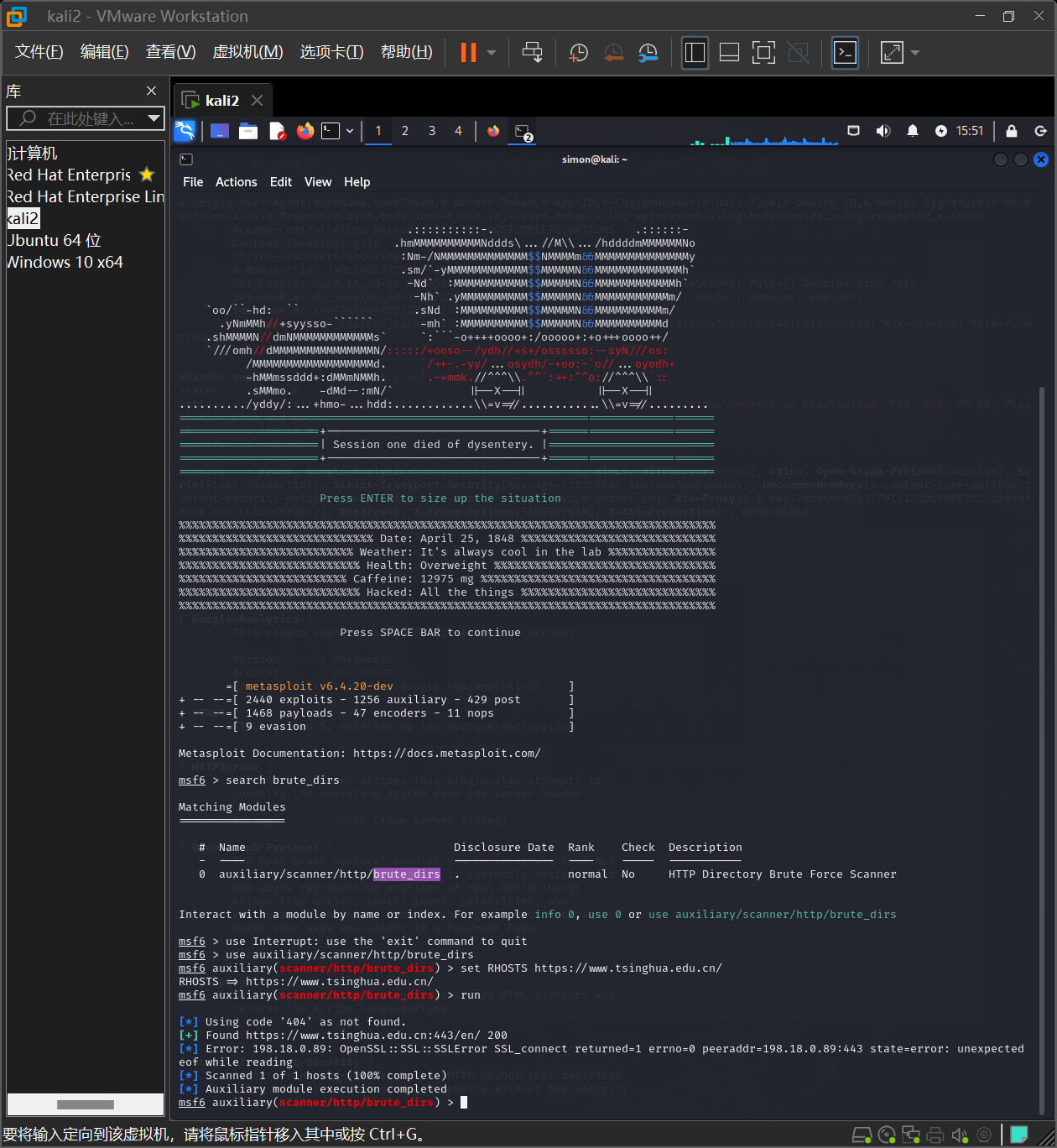
实验报告日期： 2024 年 9 月 26 日

**课程实验报告清单**

|  |
| --- |
| 目录 |
| 1.利用brute\_dirs对https://www.tsinghua.edu.cn/站点的子目录进行搜寻，并进行分析 |
| 2.对kali主机IP地址进行使用ping命令，查看其TTL值。并用nmap工具的参数命令确定自己主机的操作系统。 |
| 3.使用whatweb工具批量扫描多个网站（文件形式作为参数），包括（<https://blog.csdn.net/>，https://blog.playstation.com/），并将结果导出成111.xml文件，从结果说明blog.playstation.com/使用了什么cms框架，用了什么HTTP server？ |
| 4.利用bing搜索工具找到baidu.com域名且文件后缀为pdf的网页 |
| 5.利用harvester工具找到tsinghua.edu.cn域名下前100个邮件地址 |
| 6.使用traceroute工具查询tsinghua.edu.cn |
| 7.使用driftnet捕获并保存网站的图片，使用p0f监听主机，查看其操作系统 |
| 8.在kali上开启apache服务，让其他机器去访问该地址，使用wireshark实行监听功能查看到访问时产生的TCP三次握手记录 |
| 9.安装并使用wafw00f，检测baidu.com的防火墙是什么？ |

完成要求：必须有详细过程。

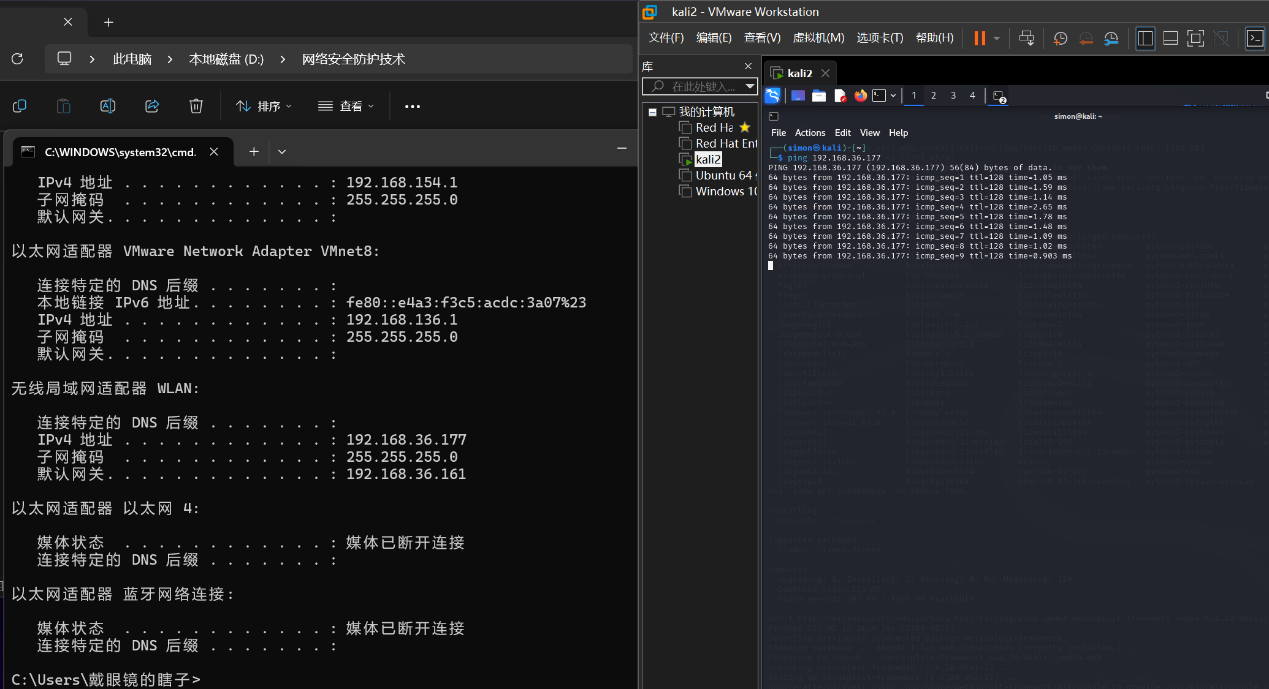
1. 利用brute\_dirs对https://www.tsinghua.edu.cn/站点的子目录进行搜寻，并进行分析



[+] Found https://www.tsinghua.edu.cn:443/en/ 200：表示成功找到一个目录 /en/，返回了 HTTP 状态码 200，说明该目录存在。

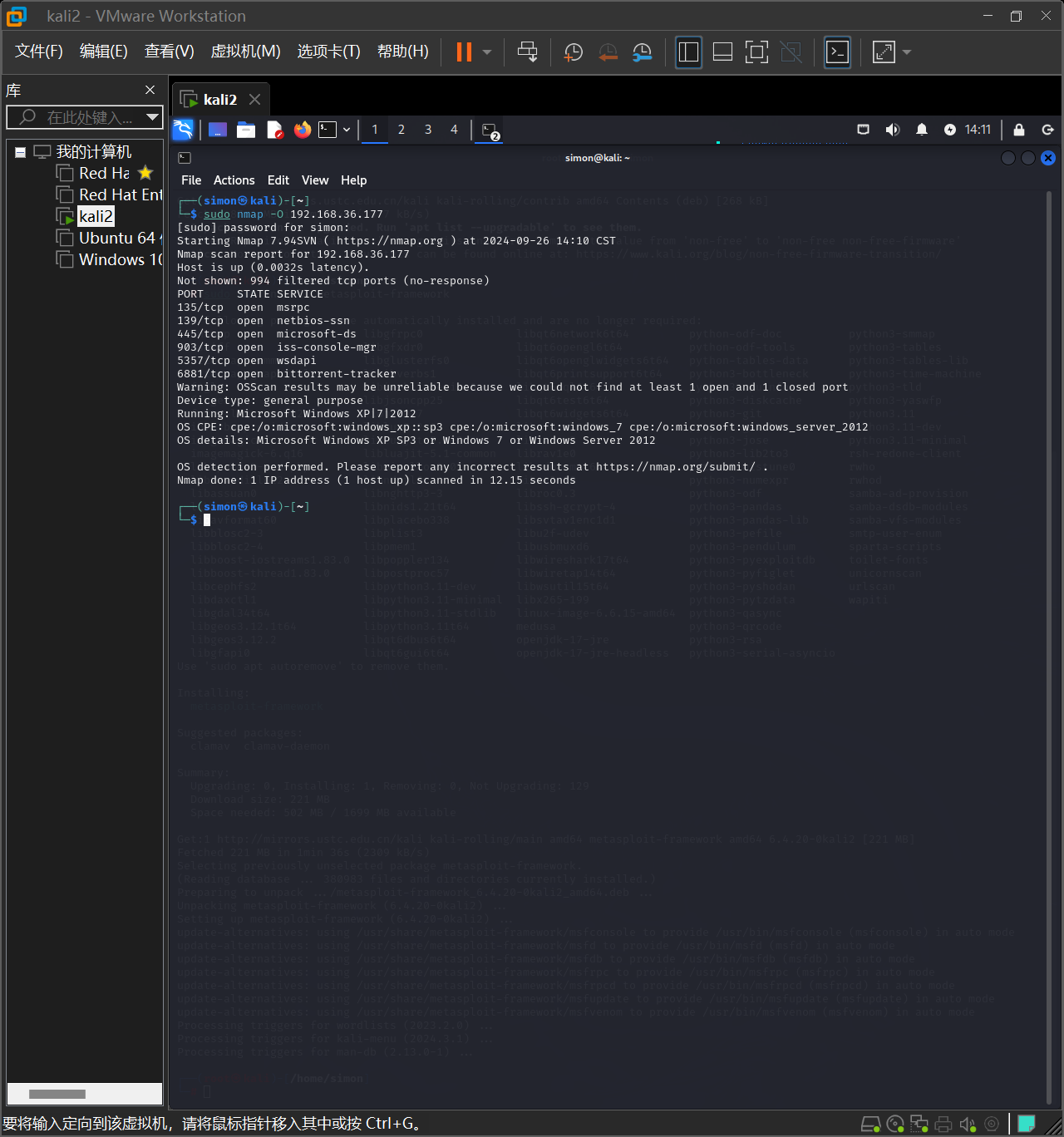
2.对kali主机IP地址进行使用ping命令，查看其TTL值。并用nmap工具的参数命令确定自己主机的操作系统。

先用一个电脑查看自己ip再用另外一个对其进行ping



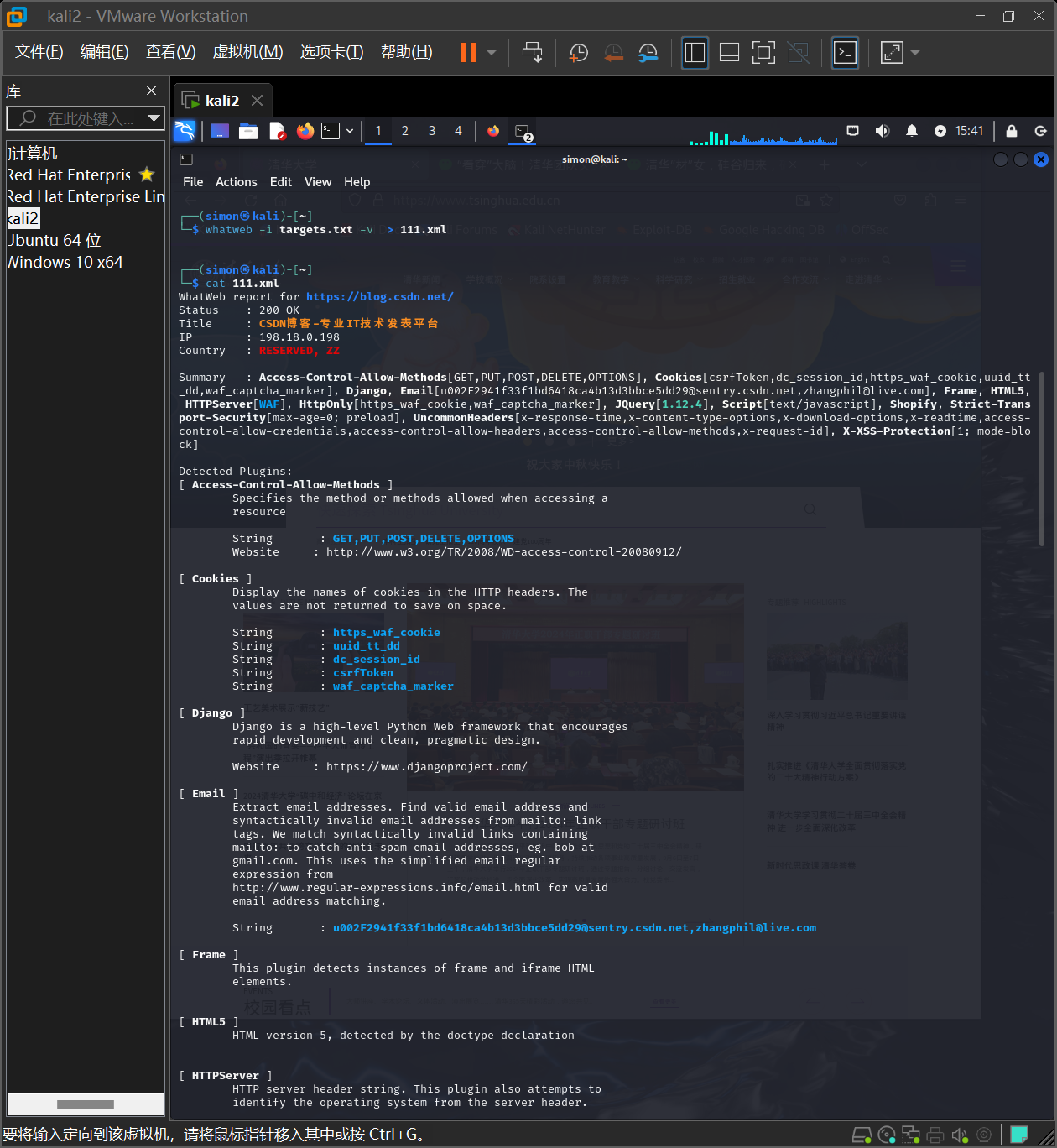
Ttl=128

用nmap进行扫描



3.使用whatweb工具批量扫描多个网站（文件形式作为参数），包括（https://blog.csdn.net/，https://blog.playstation.com/），并将结果导出成111.xml文件，从结果说明blog.playstation.com/使用了什么cms框架，用了什么HTTP server？

先把多个网站保存到target文件里 结果导出到11.xml 输出格式规范化

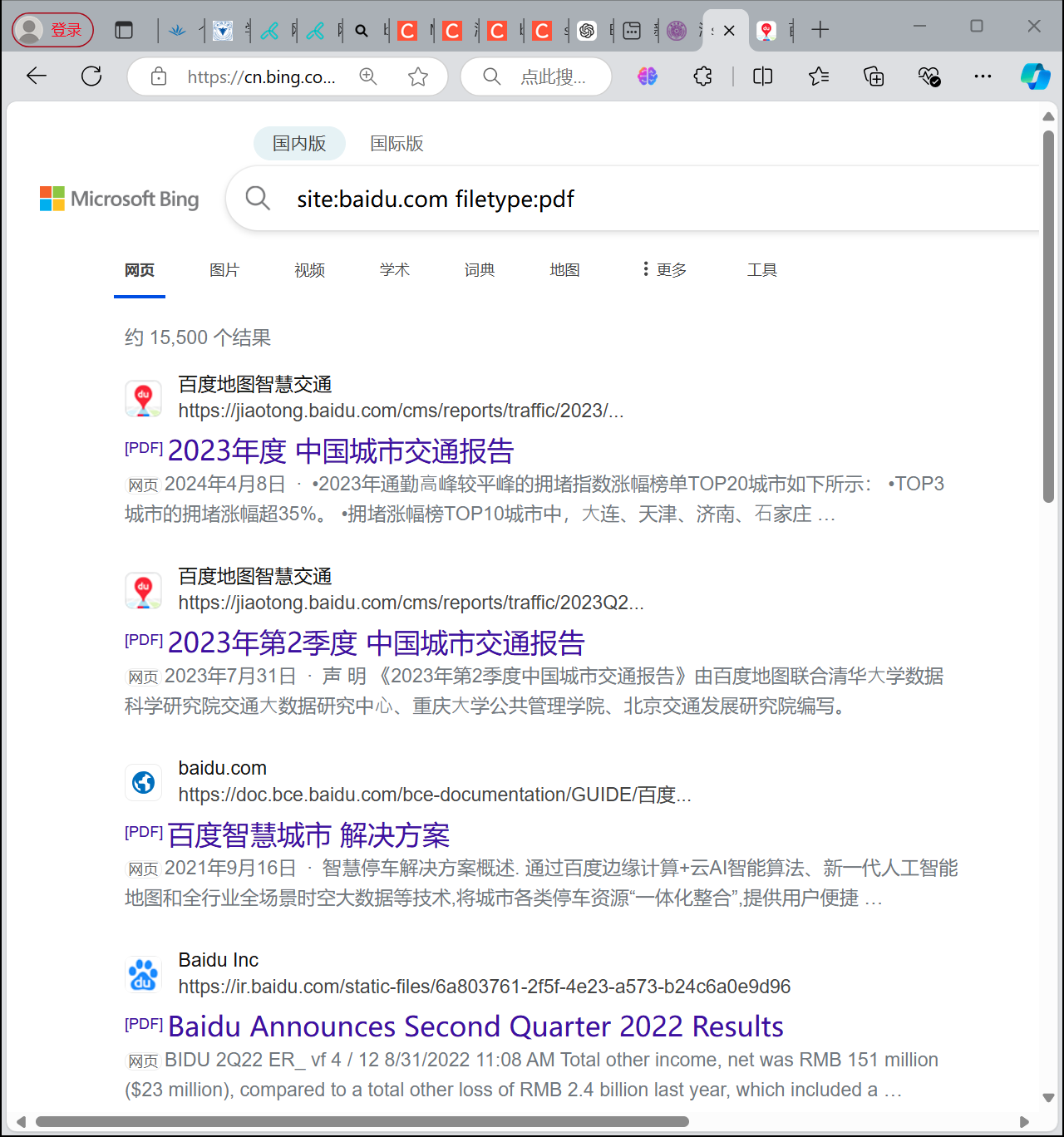


cms框架：WordPress

HTTP server：nginx

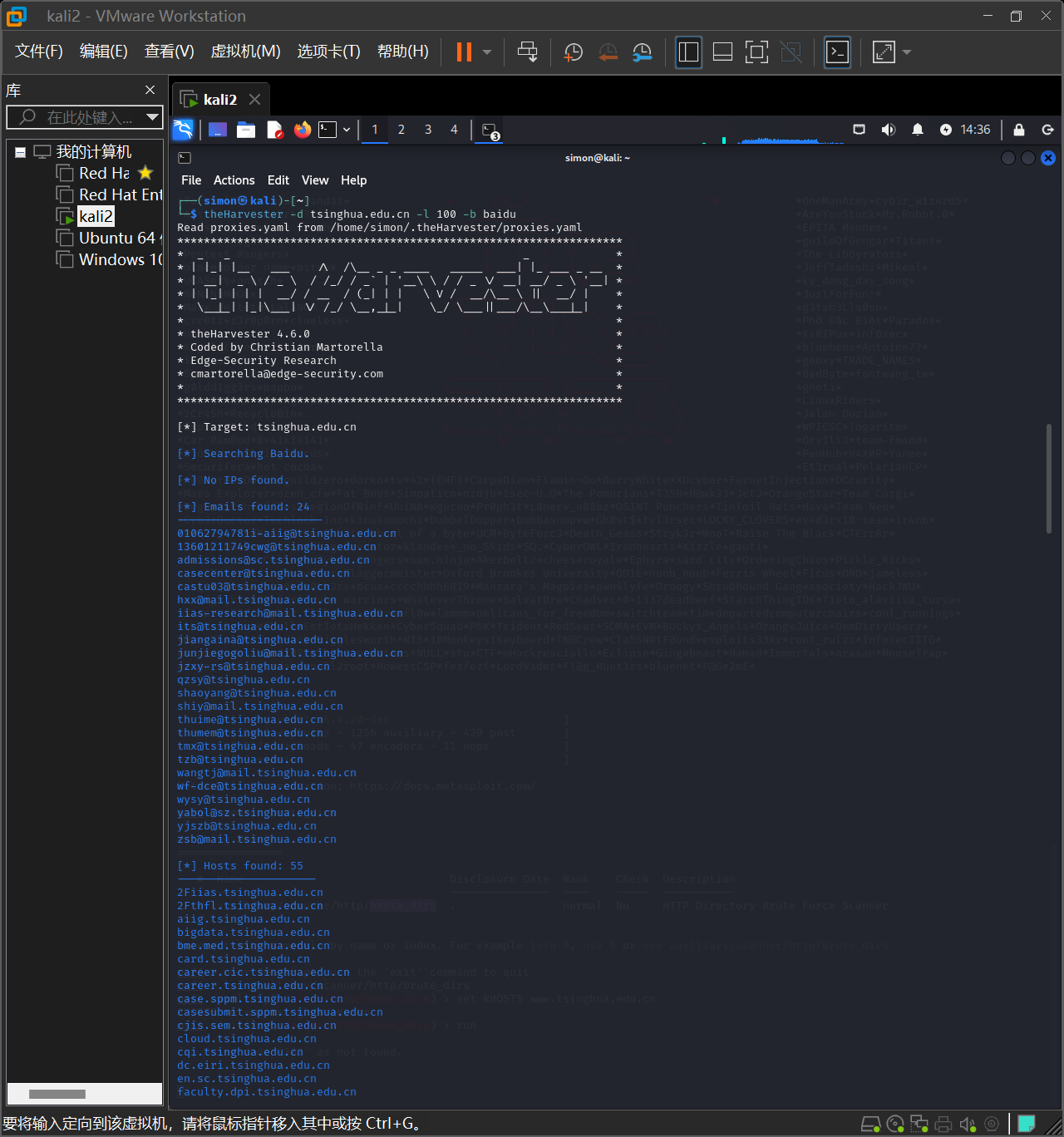
4.利用bing搜索工具找到baidu.com域名且文件后缀为pdf的网页

site:baidu.com filetype:pdf



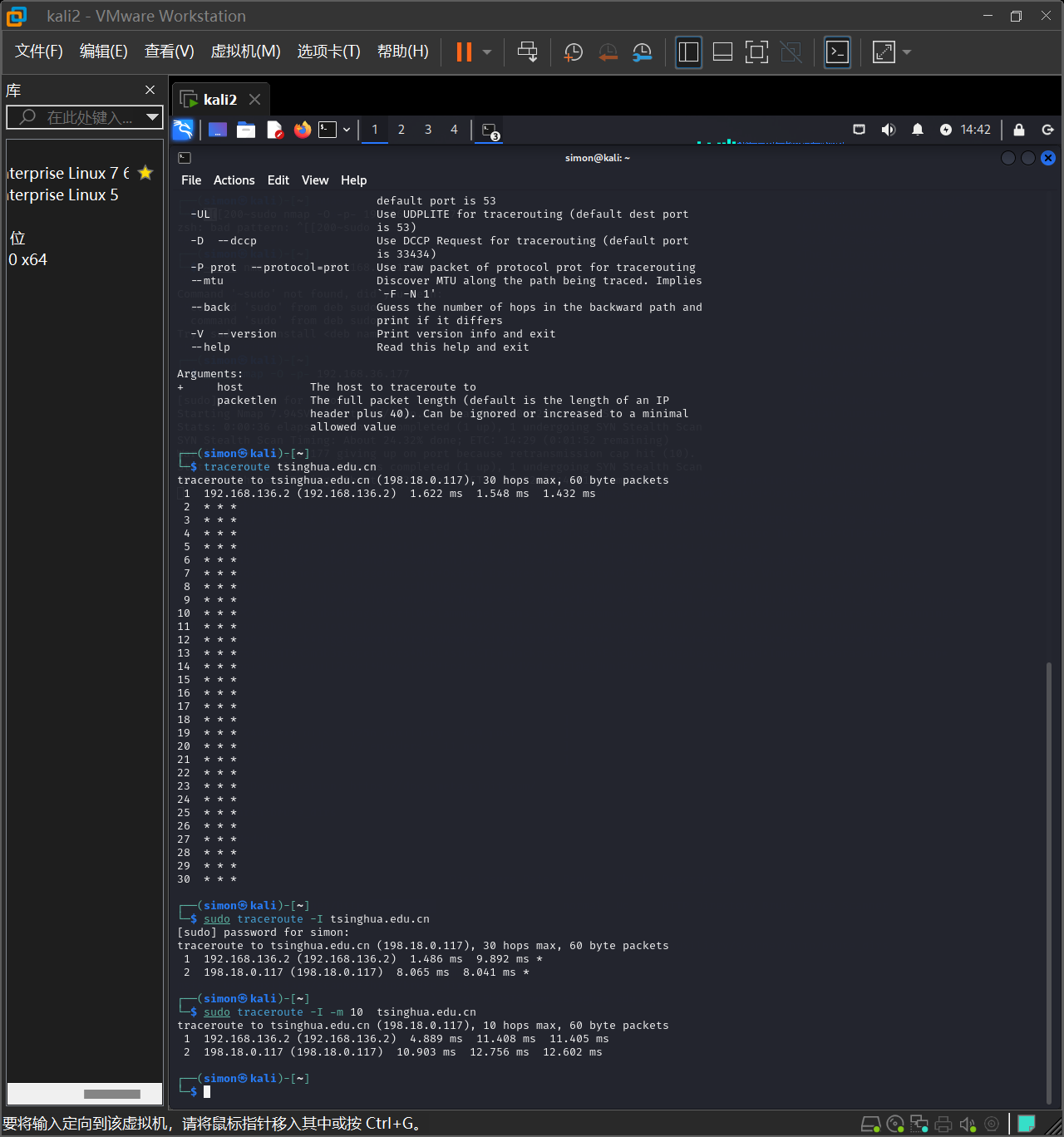
5.利用harvester工具找到tsinghua.edu.cn域名下前100个邮件地址

直接在kali里使用harvester语句进行查询



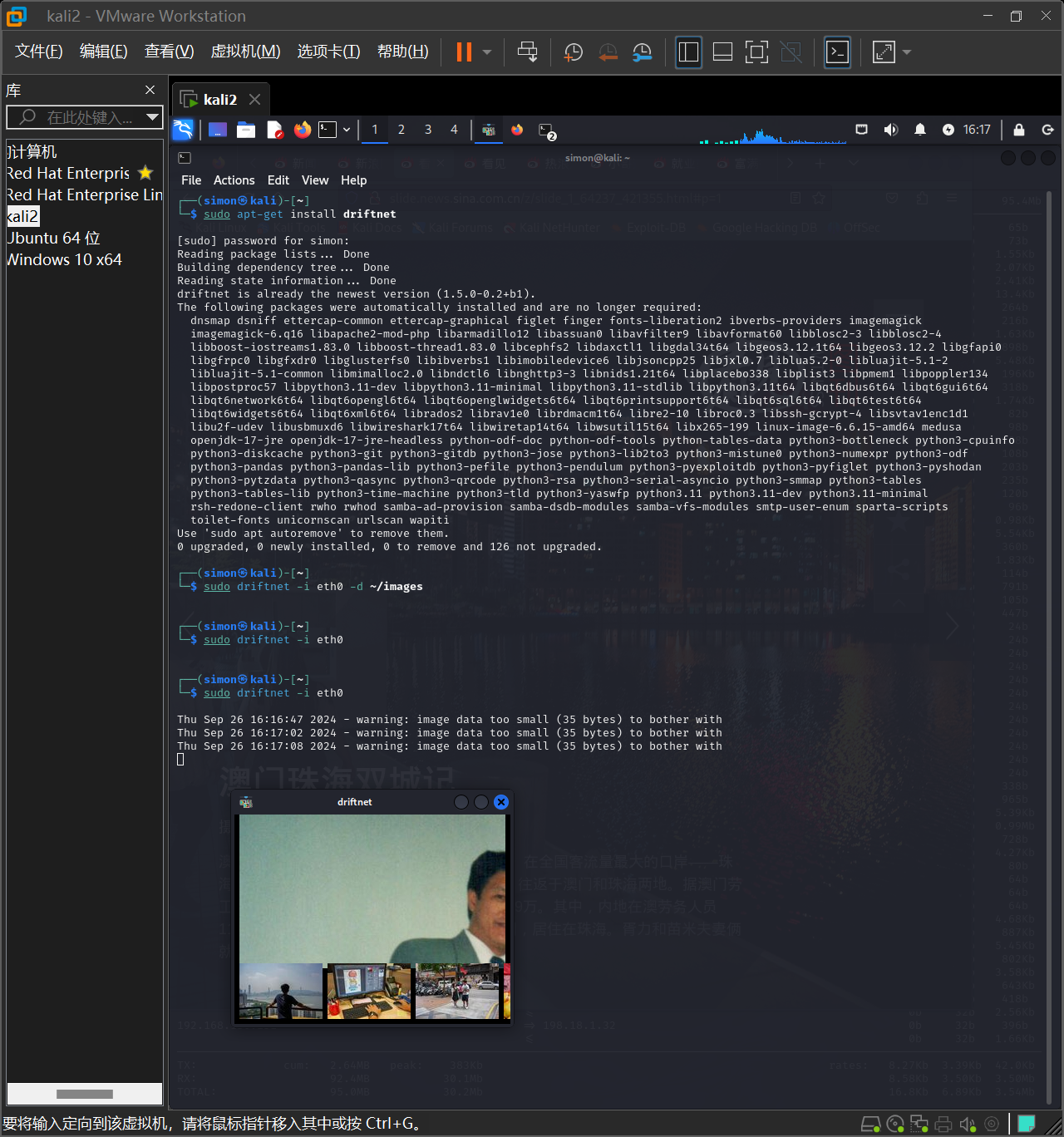
6.使用traceroute工具查询tsinghua.edu.cn

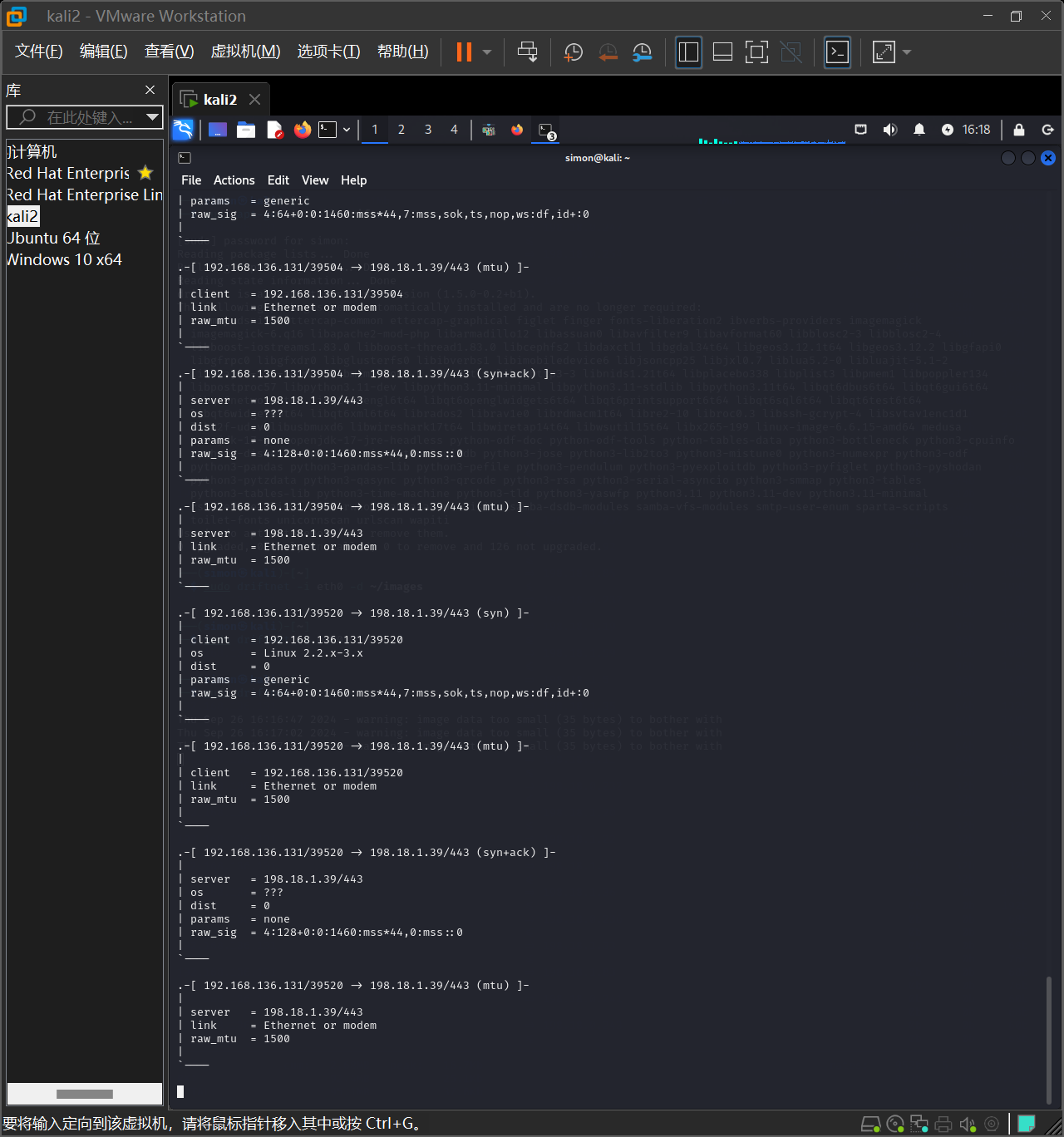
使用 traceroute -I Tsinghua.edu.cn 来进行查询



上面为结果

7.使用driftnet捕获并保存网站的图片，使用p0f监听主机，查看其操作系统





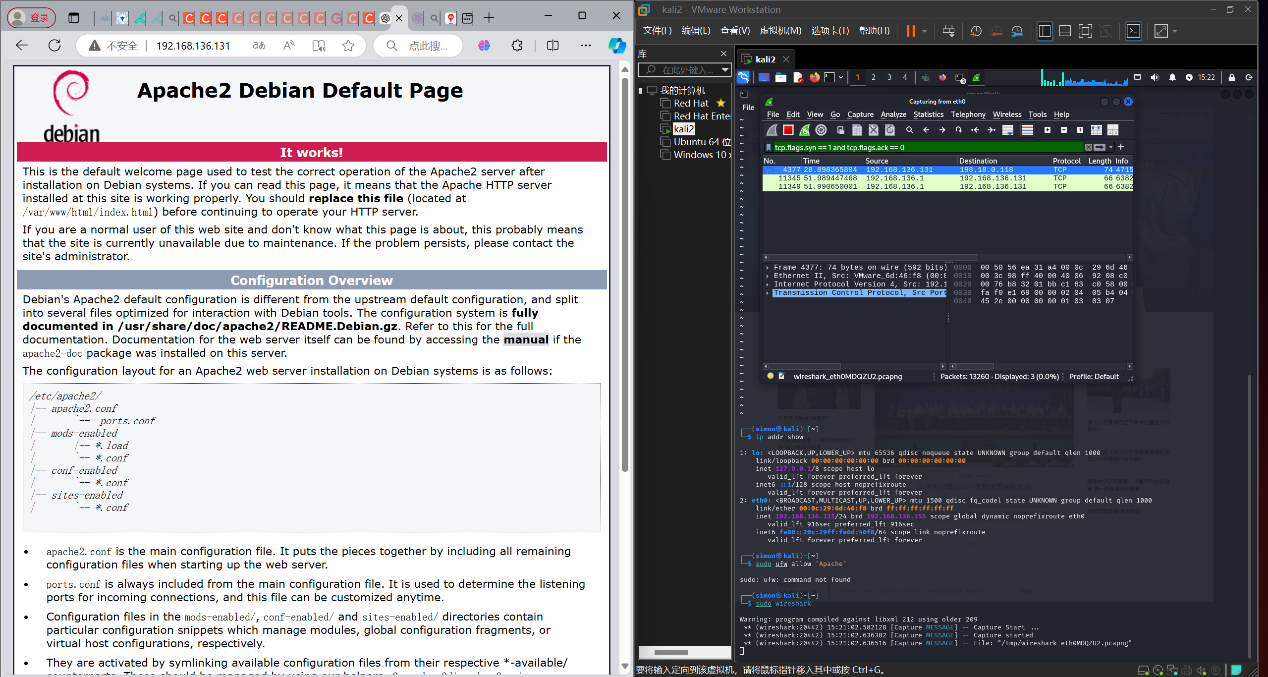
8.在kali上开启apache服务，让其他机器去访问该地址，使用wireshark实行监听功能查看到访问时产生的TCP三次握手记录

1在kali里面启动apache服务

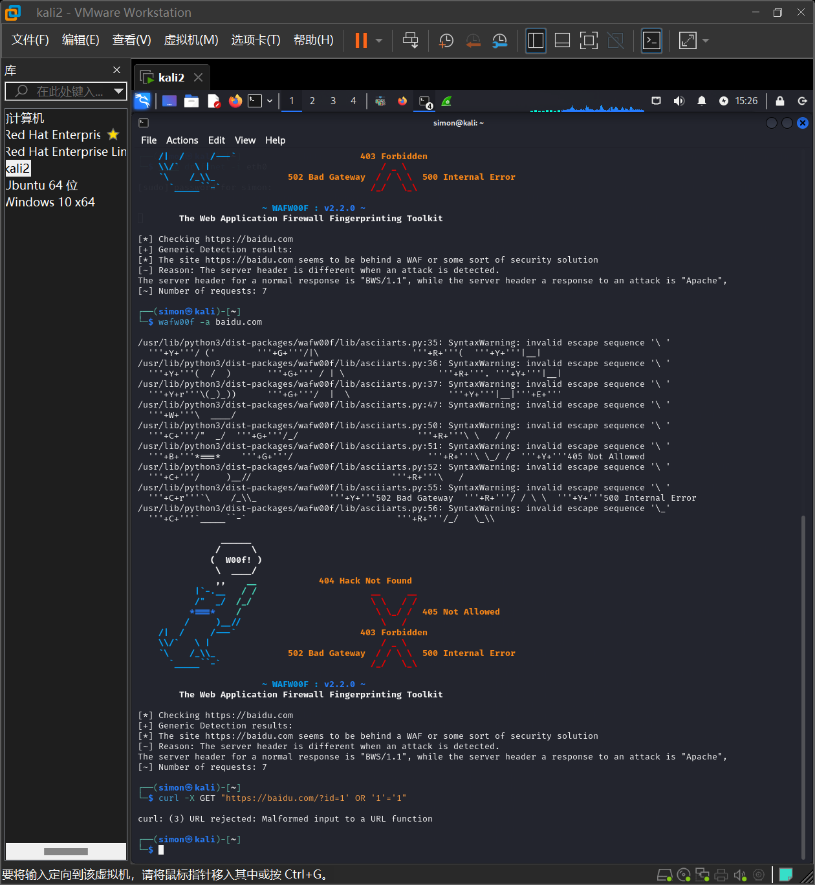
2找到kali的ip地址 192.168.136.131

3在主机浏览器直接访问kali主机

4在kali的wireshark里面过滤条件找到tcp三次握手



9.安装并使用wafw00f，检测baidu.com的防火墙是什么？



结果显示

 baidu.com 后面有 WAF，原因是当检测到攻击时，服务器的响应头有所不同。

 正常响应的服务器头是 **"BWS/1.1"**。

 对攻击的响应头则是 **"Apache"**。