**信息安全技术实验报告**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **期末考查** | |
| **组长** | **姓名** | **学号** |
|  |  |
| **组员** |  |  |
|  |  |
| 叶梓聪 | 21307417 |
| **实验分工** | | |
| **姓名** | **任务** | |
|  | 完成了XXX | |
|  |  | |
| 叶梓聪 |  | |

表1 实验拓扑中的节点名称、用户名及密码

|  |  |  |
| --- | --- | --- |
| **节点名称** | **用户名** | **密码** |
| Web服务器 | root | root |
| 本地DNS | root | root |
| 外网权威DNS | root | root |
| 学生主机 | kali | kali |
| 教务老师主机 | administrator | admin |
| 外网攻击者主机 | kali | kali |

【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+实验名称命名

# 实验目的与实验内容

## 1.1 实验目的

* 了解网络入侵检测与防御系统的基本功能、部署位置；
* 掌握常用且开源的网络入侵检测与防御系统Snort在局域网（如公司网络、学校网络等）中的配置方法；
* 理解并掌握Web安全技术，特别是Web SQL注入攻击原理、过程和防御技术；
* 掌握Snort的检测与防御规则的配置方法；
* 理解DNS重要性，掌握为一个公司或企业注册域名的过程和方法；
* 回顾和巩固在课堂教学、12个课堂实验+6个期末实验中学习到的网络安全知识、网络攻击和防御技术，用所学知识实现具体场景的安全防御。

## 实验内容

### 1.2.1 实验1：安全检测与防御系统Snort的基本配置

主要实验内容：

* 查看网络拓扑并确定内网边界
* 将Snort配置为网关

### 1.2.2 实验2：Web SQL注入攻击

主要实验内容：

* 寻找SQL攻击注入点
* 确定注入点是否可注入
* 确定表的查询列数
* 使用union确定注入的显示位置
* 泄露内网数据库的数据
* 测试登录页面的SQL注入漏洞
* 布尔盲注

### 1.2.3 实验3：防御Web SQL注入攻击

主要实验内容：

* 配置snort检测系统

创建规则文件

开启inline模式

* 编写Snort规则、实现对Web SQL注入攻击的检测

编写Snort规则

令编写的规则生效

验证防御效果

使用drop命令阻止SQL注入查询

### 1.2.4 实验4：DNS配置与应用

主要实验内容：

* 添加本地域名www.localhost

配置本地DNS

令配置生效

验证本地注册的域名的有效性

* 注册可访问域名www.sysu

### 1.2.5 实验5：具体场景下的安全防御策略实现

主要实验内容：具体场景下的安全防御策略实现

在防火墙网关机器上，配置其另外两块网卡，连接外网权威DNS和外网攻击者，使用iptables或netfilter或配置snort规则，实现如下防御策略：

* 外网攻击者无法访问任意内网设备（包括web服务器，本地DNS，教务老师主机，学生主机），但可访问外网权威DNS。并证明防御的有效性。
* 教务老师主机可以访问web服务器上的教务系统，学生无法访问web服务器。
* 设置本地DNS请求限制，限制任何客户端请求速度不得超过 5次/10秒。

# 实验步骤与实验结果记录

### 实验1：安全检测与防御系统Snort的基本配置

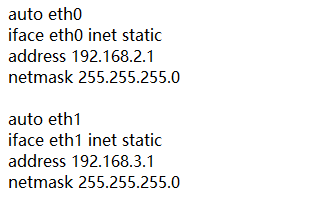
主要实验内容：

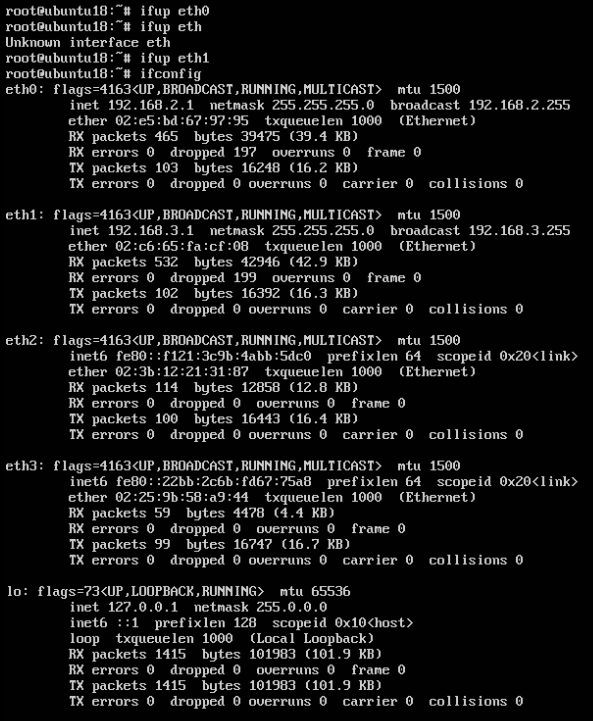
* 查看网络拓扑并确定内网边界
* 将Snort配置为网关

1、确定内网边界为防火墙网关

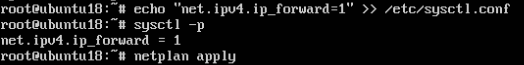
2、将Snort配置为网关

（1）配置防火墙网关机器的网卡

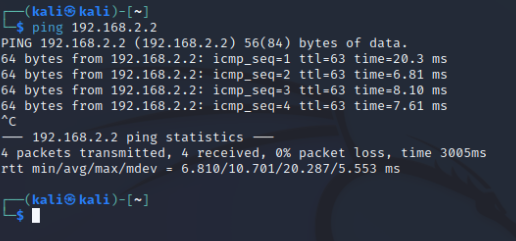




（2）开启IPv4转发，并重启网络服务使其生效



（3）验证网络连通性

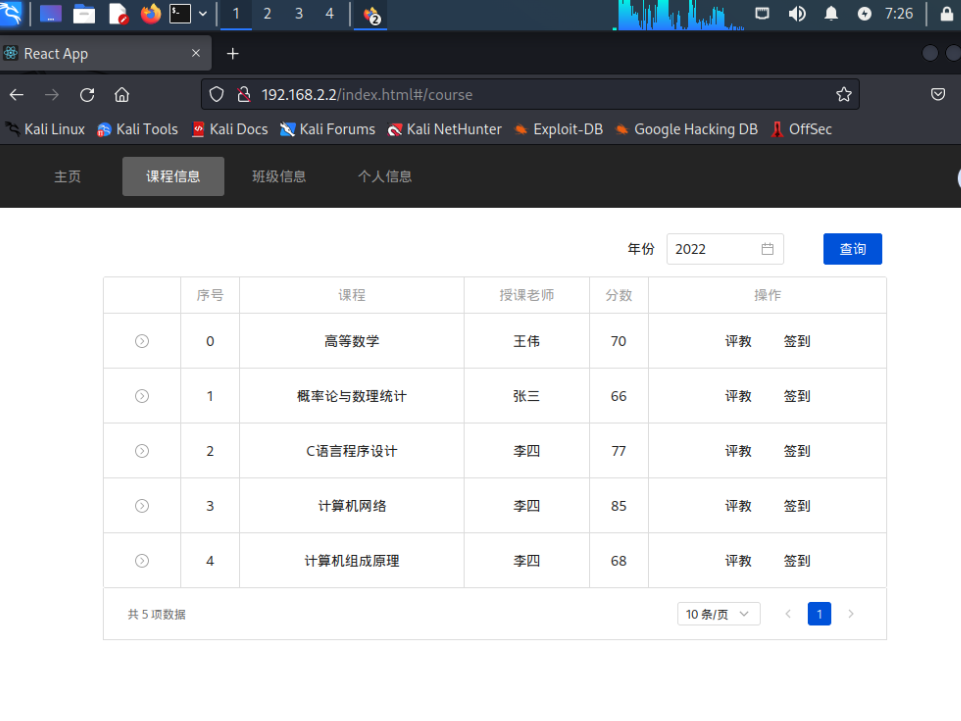


### 实验2：Web SQL注入攻击

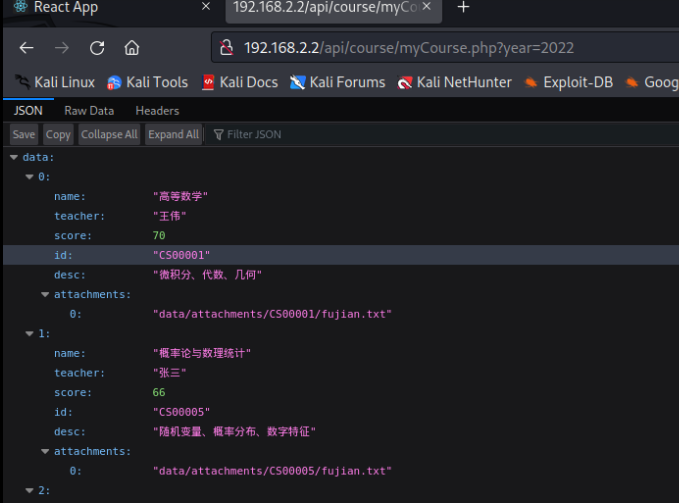
主要实验内容：

* 寻找SQL攻击注入点
* 确定注入点是否可注入
* 确定表的查询列数
* 使用union确定注入的显示位置
* 泄露内网数据库的数据
* 测试登录页面的SQL注入漏洞
* 布尔盲注

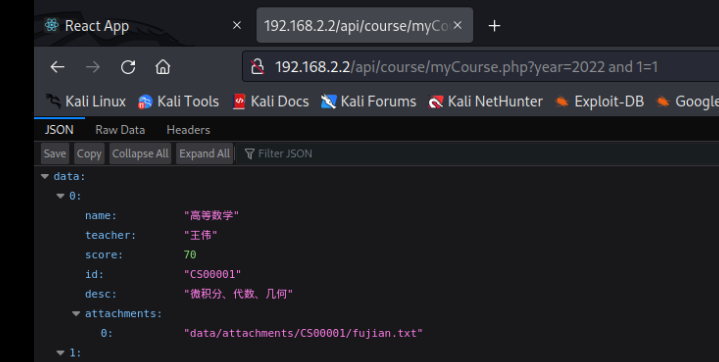
1、测试教务系统服务

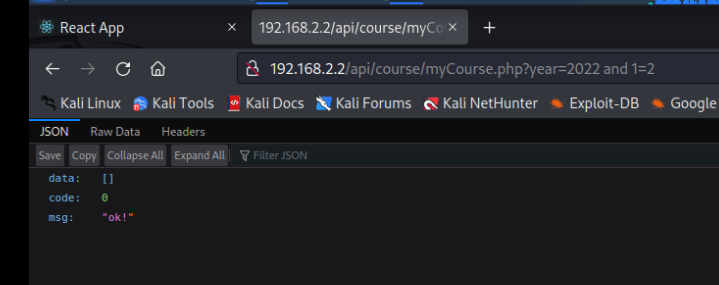


2、寻找SQL攻击注入点

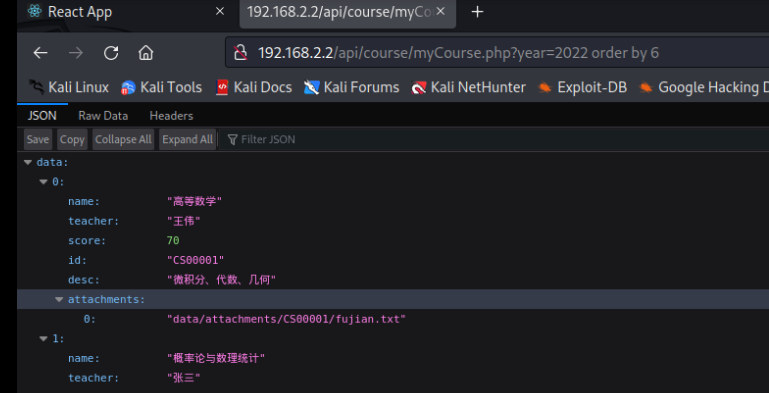


3、确定注入点是否可注入

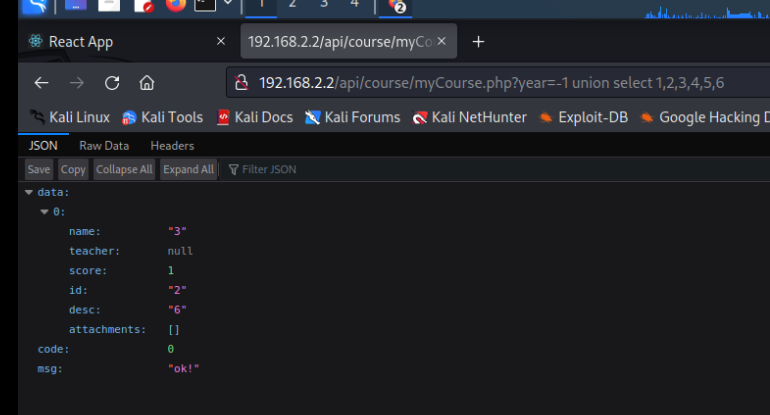




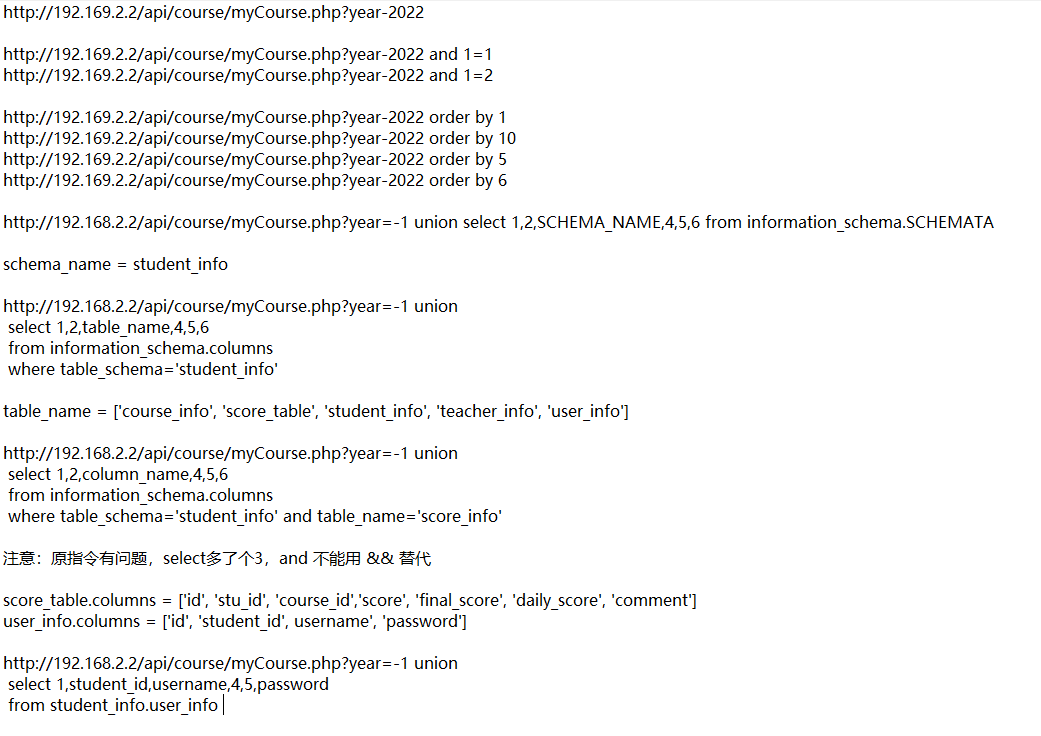
4、确定表的查询列数



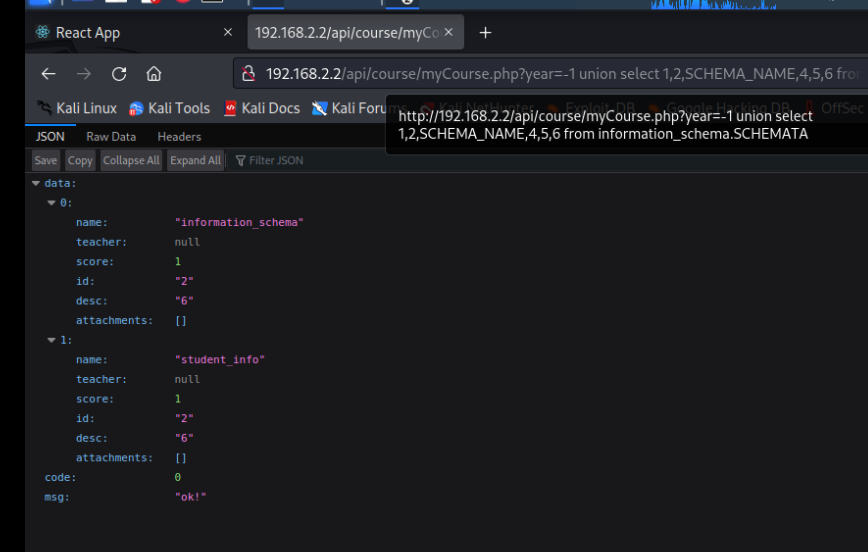
5、使用union确定注入的显示位置



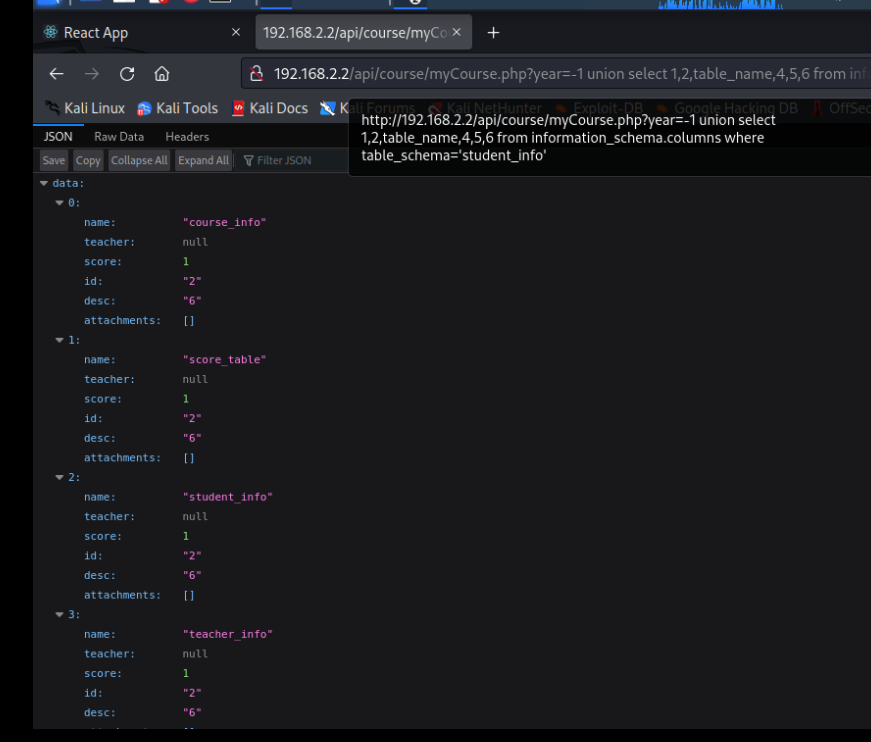
6、非法获取内网数据库的数据



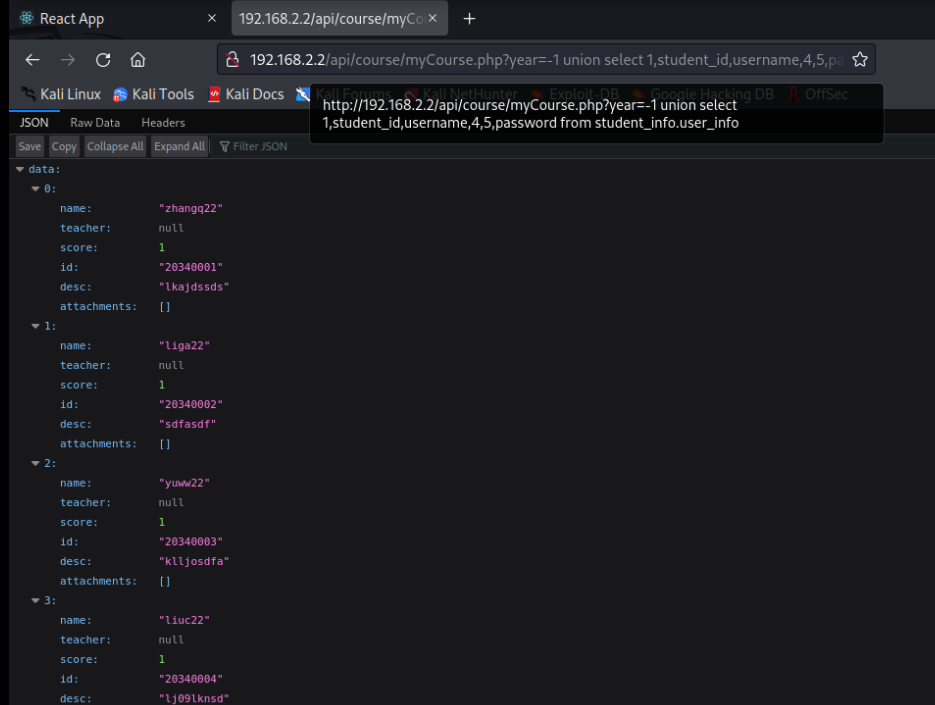
（1）列出所有数据库



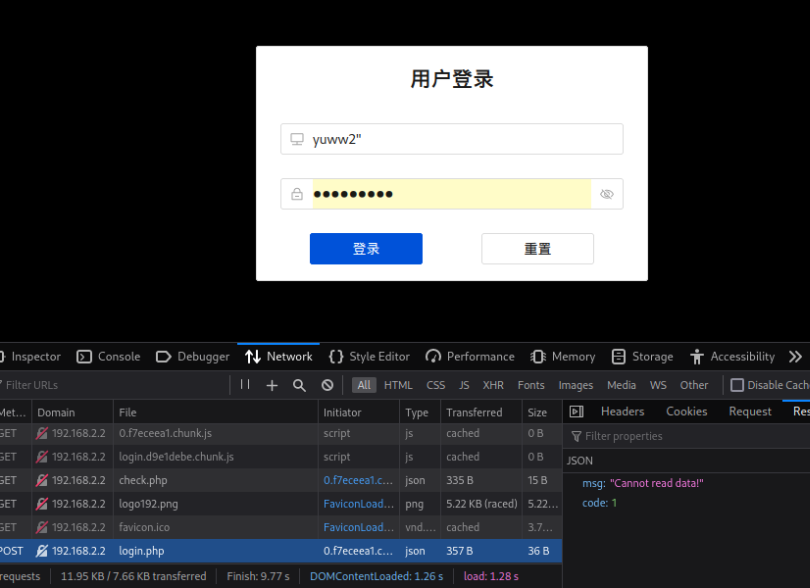
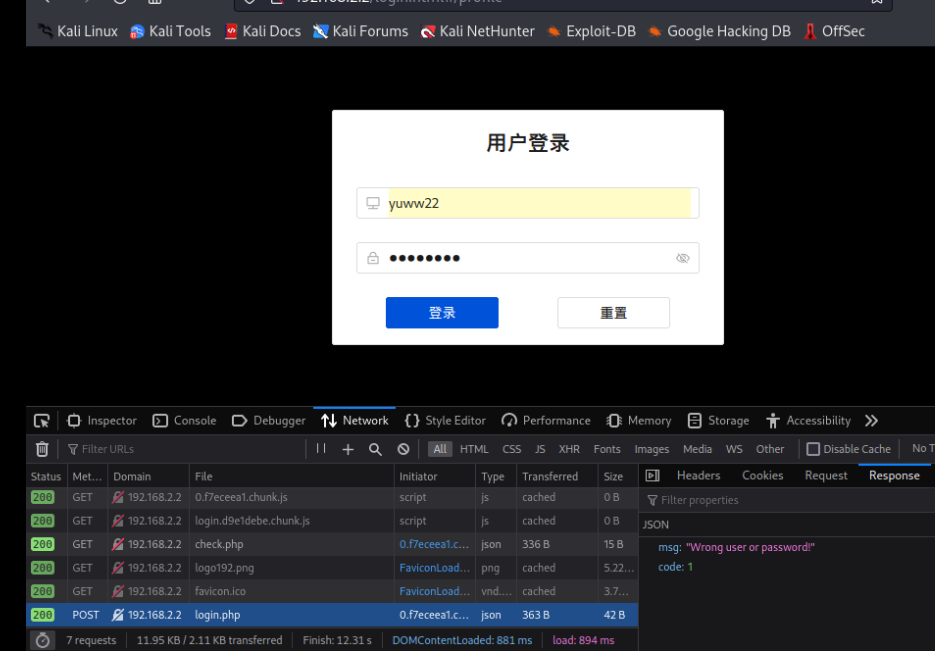
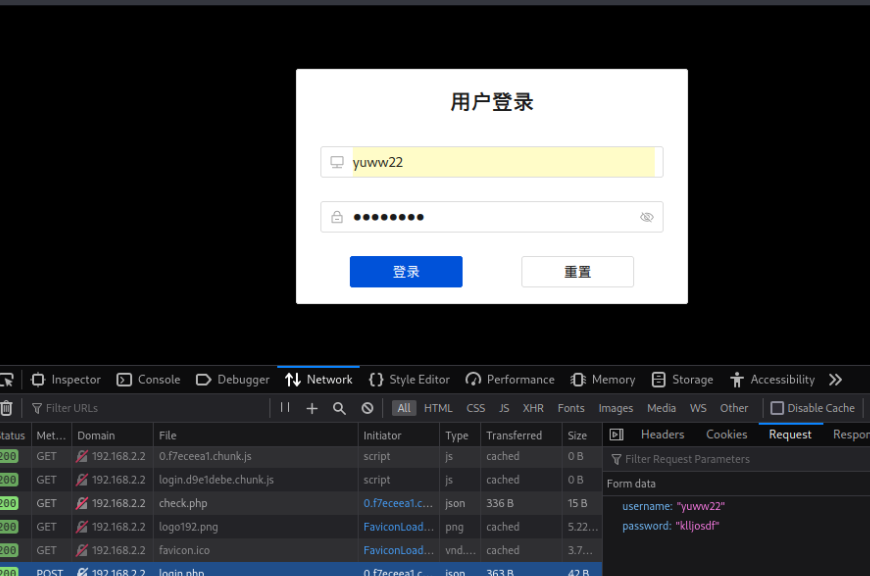
（2）列出所有数据表



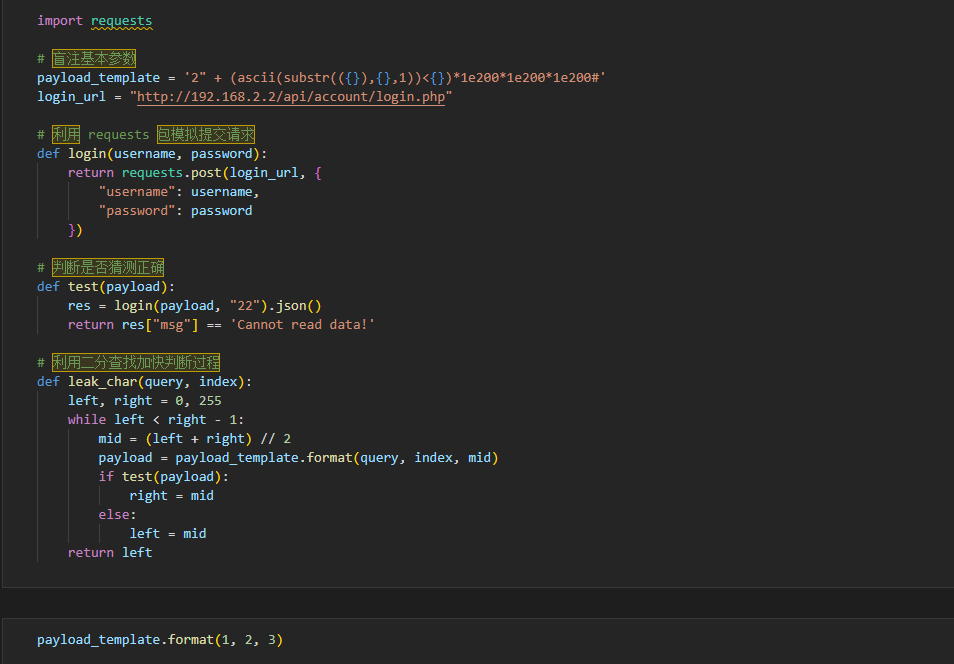
（4）非法获取想要的数据

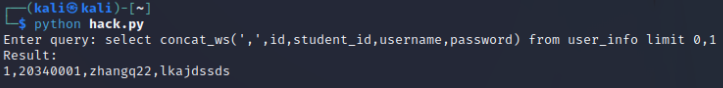


7、测试登录页面的SQL注入漏洞



（8）布尔盲注





### 实验3：防御Web SQL注入攻击

主要实验内容：

* 配置snort检测系统

创建规则文件

开启inline模式

* 编写Snort规则、实现对Web SQL注入攻击的检测

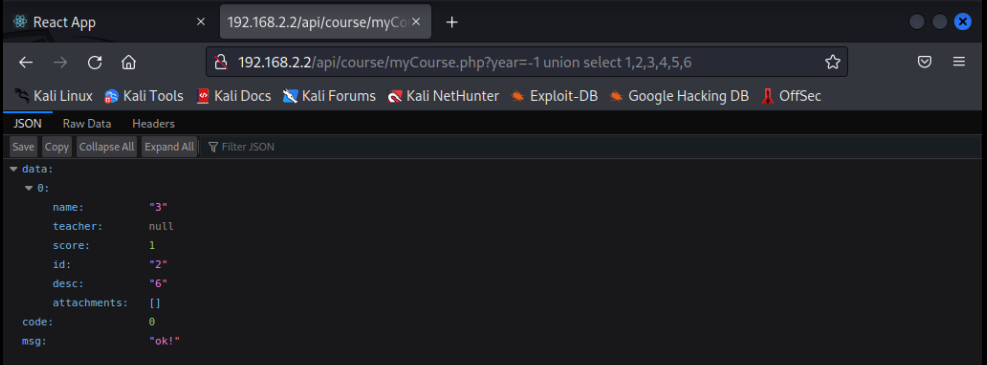
编写Snort规则

令编写的规则生效

验证防御效果

使用drop命令阻止SQL注入查询

1、测试教务系统服务

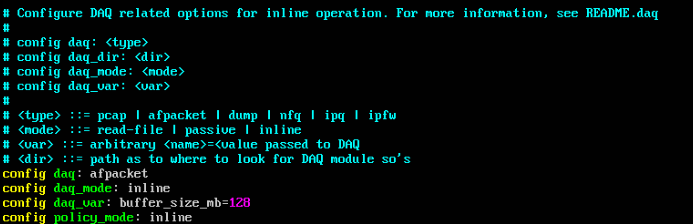


2、配置snort检测系统

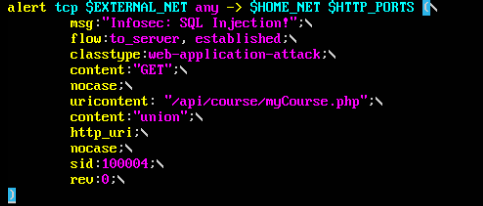
（1）创建规则文件

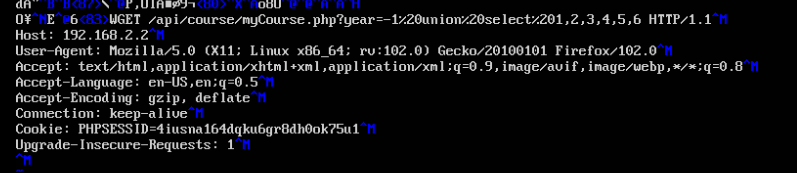


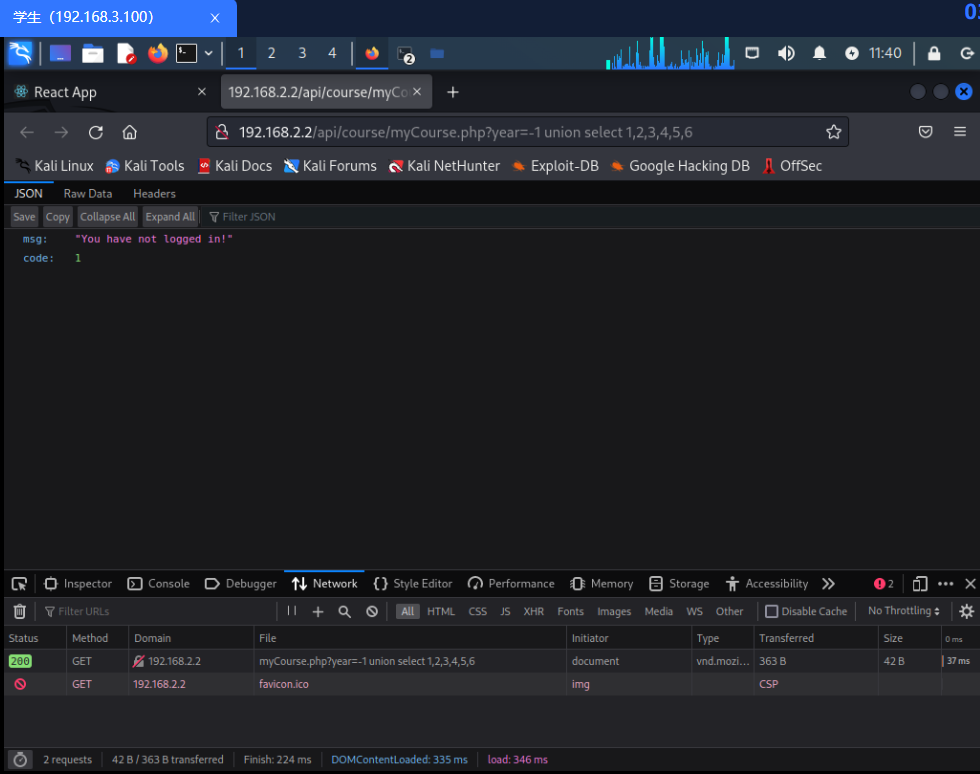
（2）开启inline模式

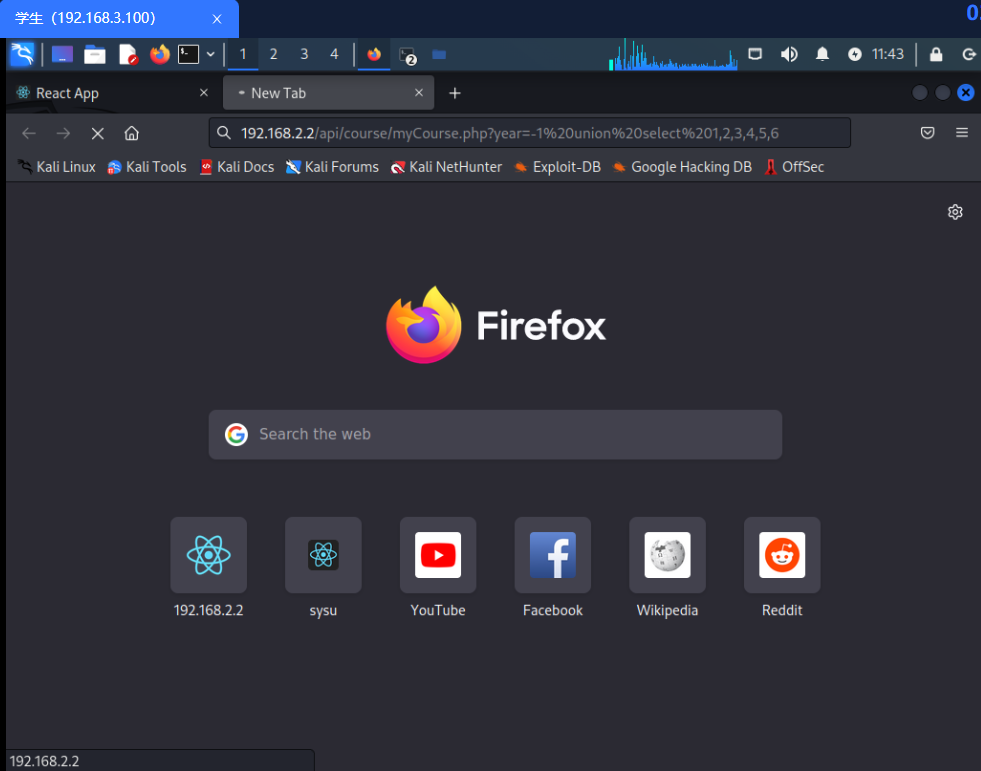


3、编写Snort规则，实现对Web SQL注入攻击的检测









### 实验4：DNS配置与应用

主要实验内容：

* 添加本地域名www.localhost

配置本地DNS

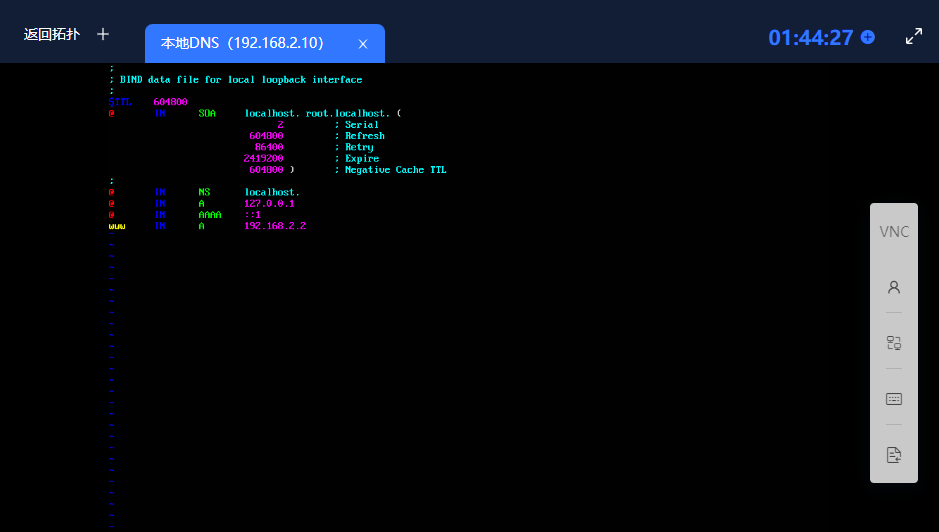
令配置生效

验证本地注册的域名的有效性

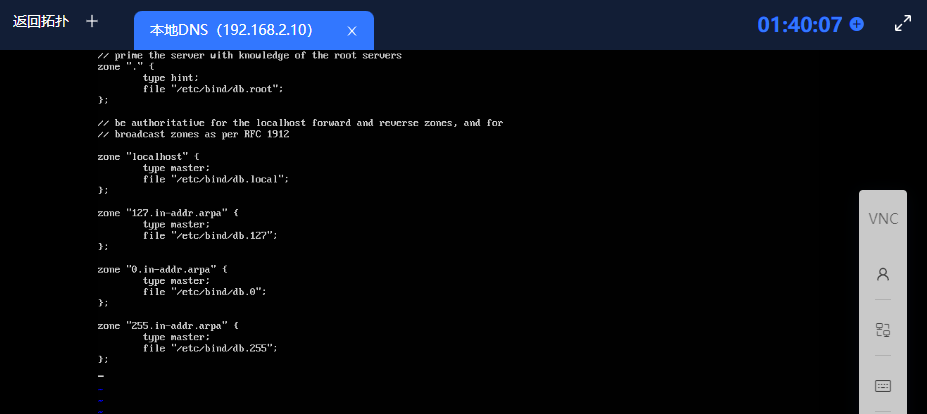
* 注册可访问域名www.sysu

1、添加本地域名www.localhost

（1）配置本地DNS



（2）

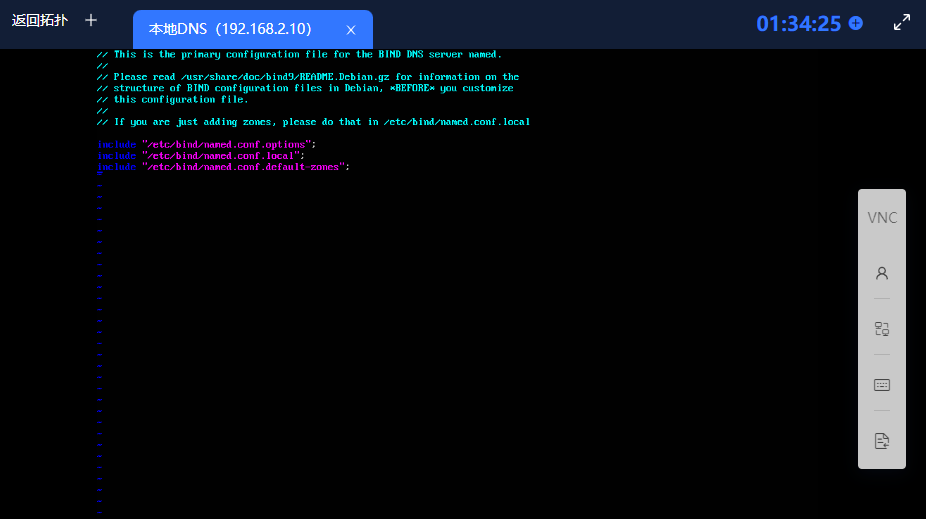


named.conf.default-zones用于默认的DNS区域配置。

Zone “localhost”: 定义一个名为localhost的DNS区域，区域是DNS配置的基本单元，每个区域对应一个域名空间。

type master：指定区域的类型为master（主），主区域的DNS服务器拥有该区域的原始数据，并负责该区域的权威解析。

file “path”：指定存放该区域数据的文件路径。



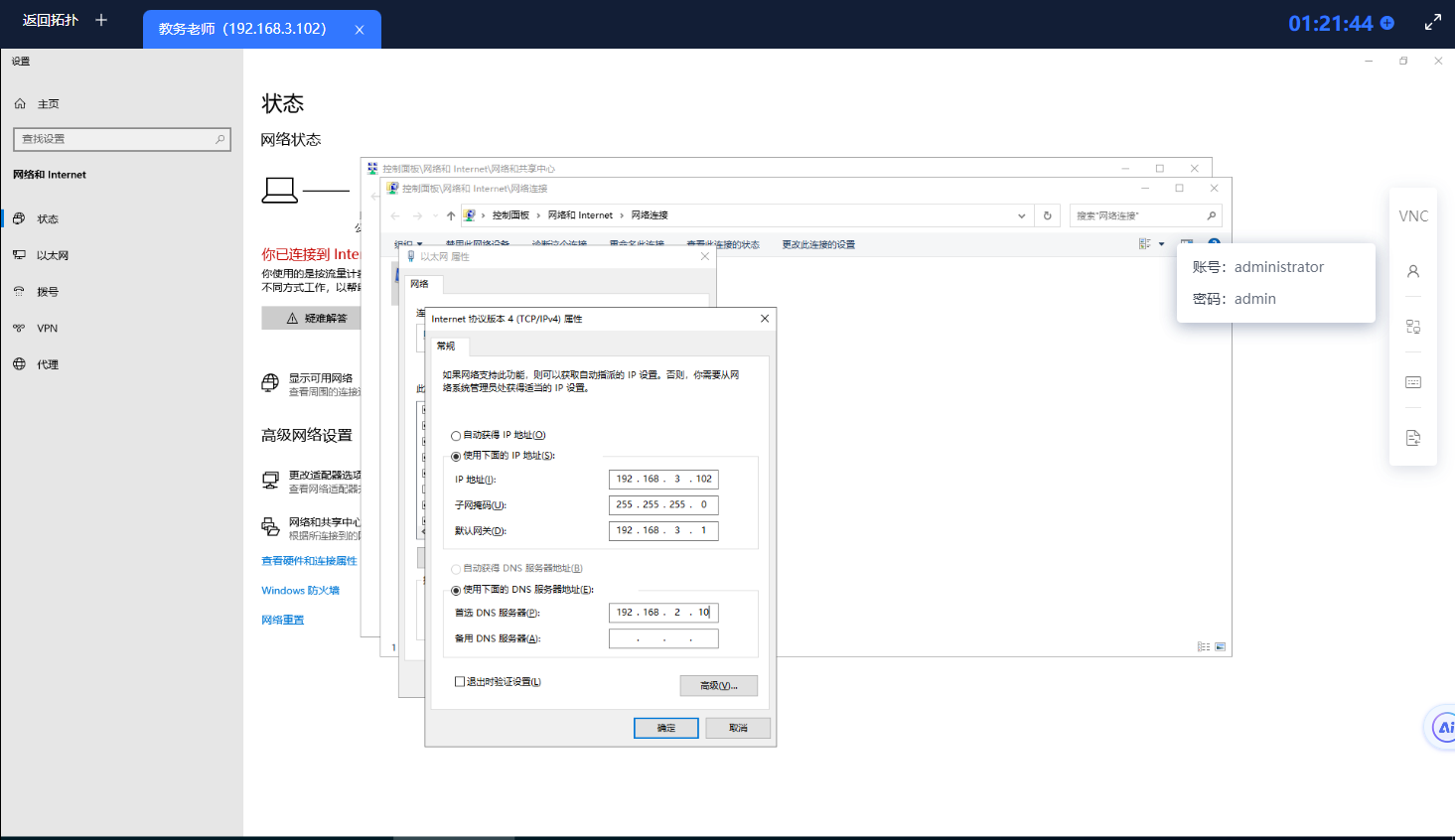
这些指令告诉BIND9加载并包含其他配置文件中的内容，指示BIND9包含这三个文件中的配置。

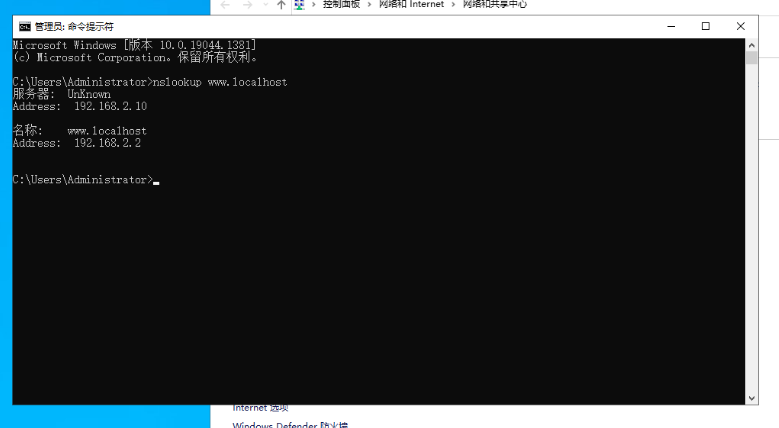
（3）令配置生效



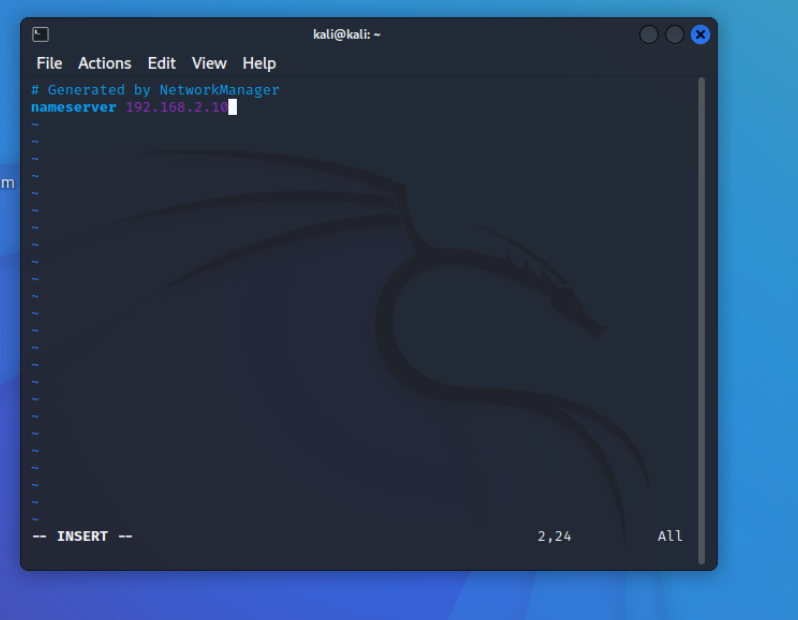
（4）验证本地注册的域名的有效性

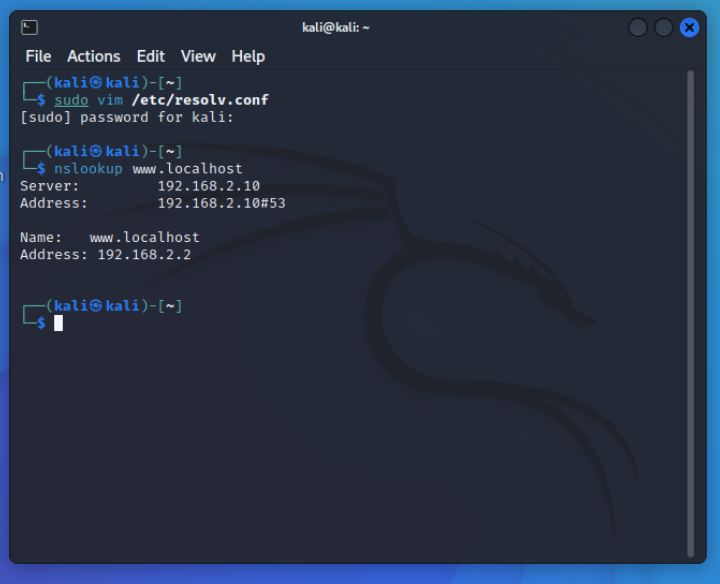
设置教务老师的域名解析服务器为192.168.2.10

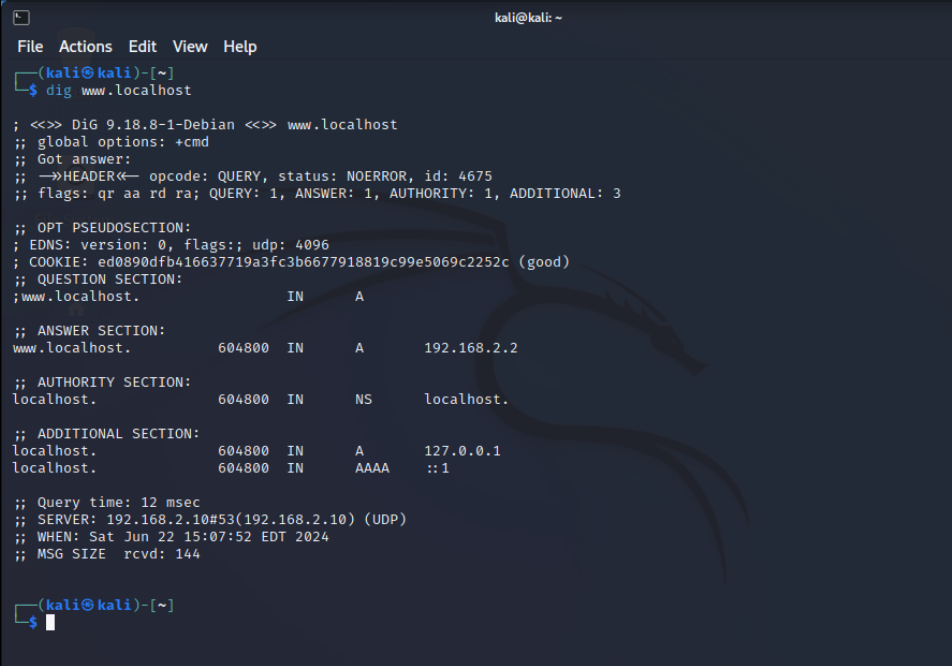




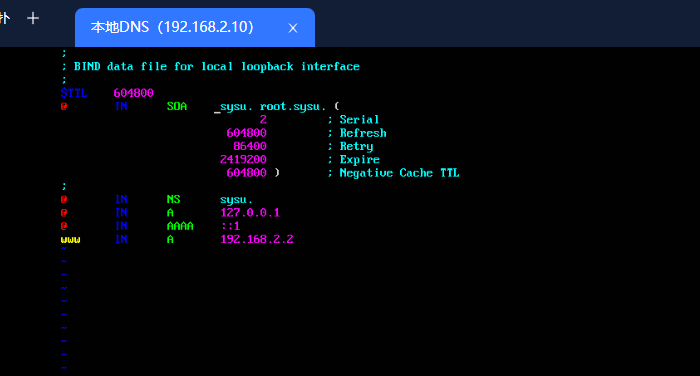
设置学生主机的域名解析器

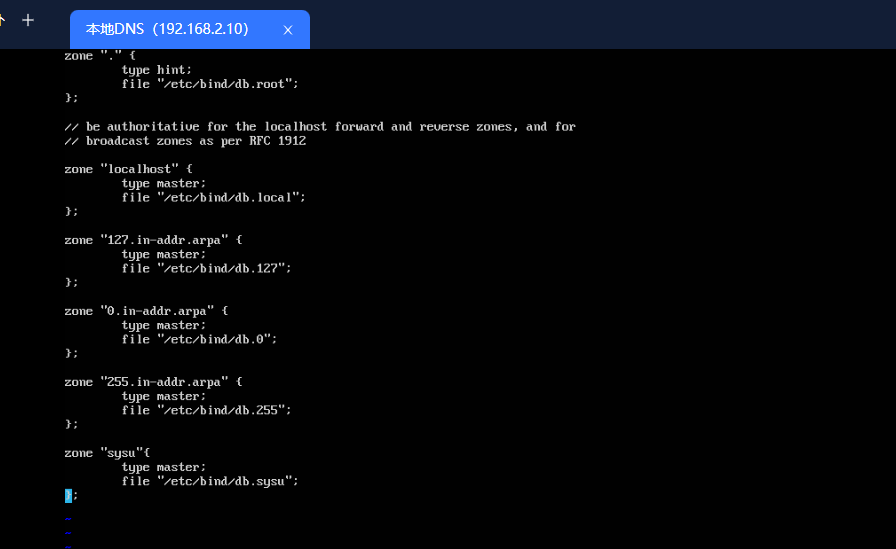


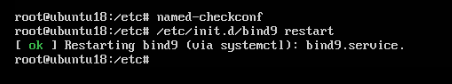




2、注册可访问域名[www.sysu](http://www.sysu)

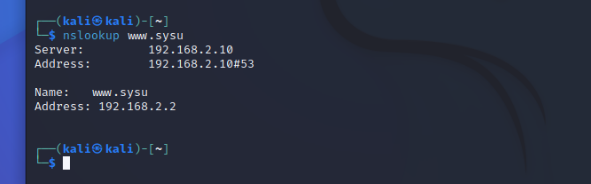


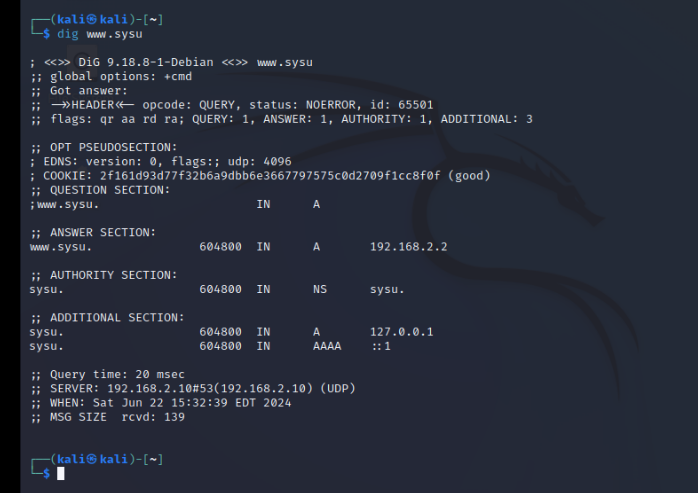




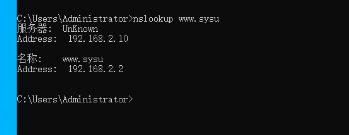
验证

学生主机





教师主机



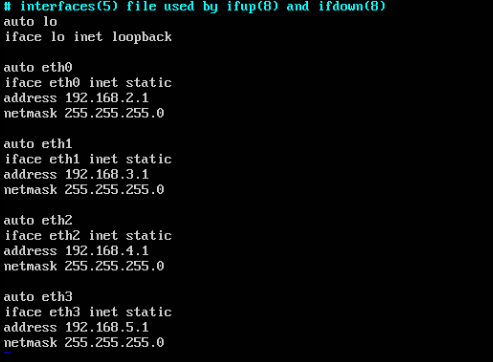
### 实验5：具体场景下的安全防御策略实现

主要实验内容：具体场景下的安全防御策略实现

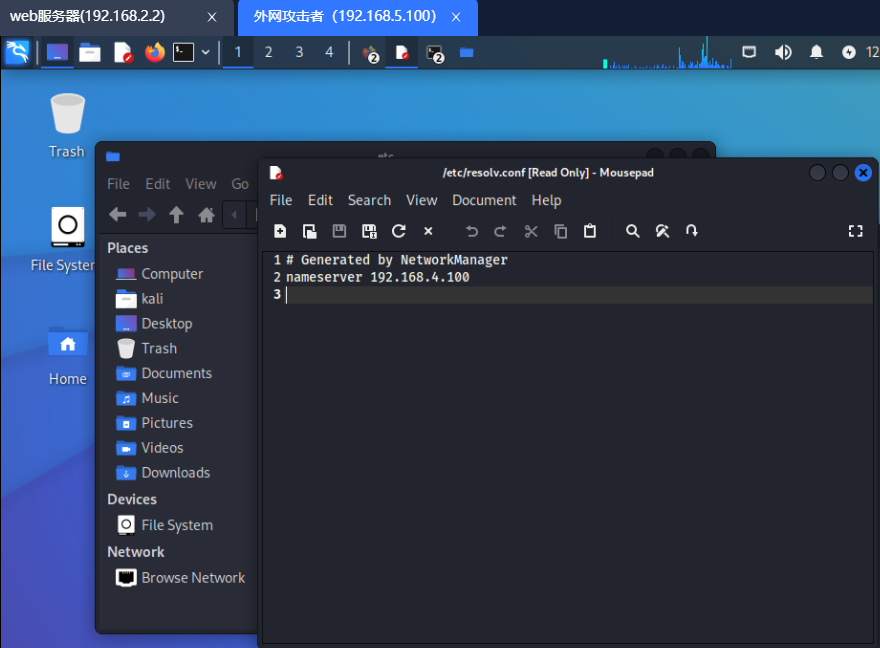
在防火墙网关机器上，配置其另外两块网卡，连接外网权威DNS和外网攻击者，使用iptables或netfilter或配置snort规则，实现如下防御策略：

* 外网攻击者无法访问任意内网设备（包括web服务器，本地DNS，教务老师主机，学生主机），但可访问外网权威DNS。并证明防御的有效性。
* 教务老师主机可以访问web服务器上的教务系统，学生无法访问web服务器。
* 设置本地DNS请求限制，限制任何客户端请求速度不得超过 5次/10秒。

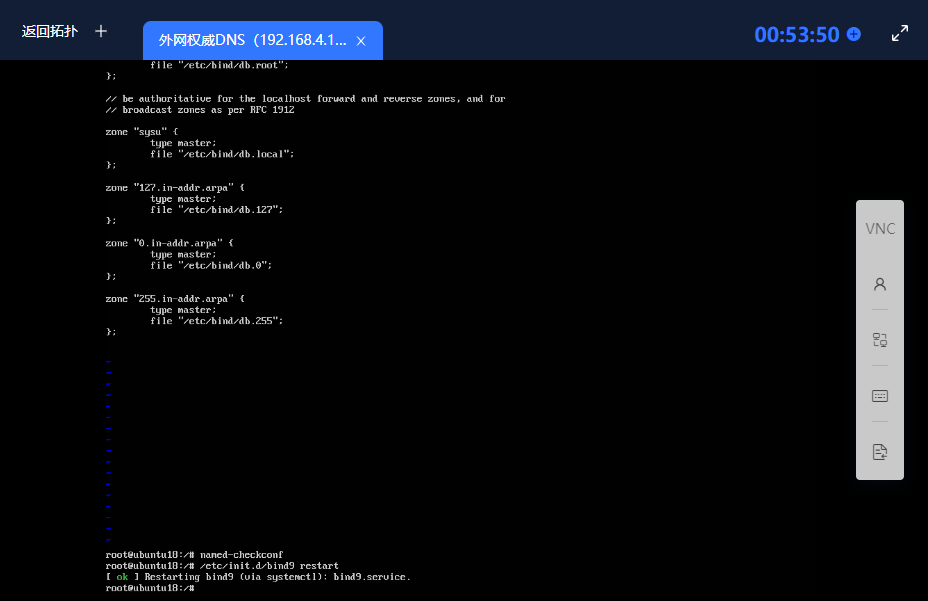
1、配置网关服务器端口



2、修改攻击者主机/etc/resolv.conf文件



3、配置外网权威域名服务器


4、攻击者主机上进行验证www.sysu



5、配置防火墙网关实现防御策略

sudo iptables -A FORWARD -s 192.168.5.0/24 -d 192.168.2.0/24 -j DROP

sudo iptables -A FORWARD -s 192.168.5.0/24 -d 192.168.3.0/24 -j DROP

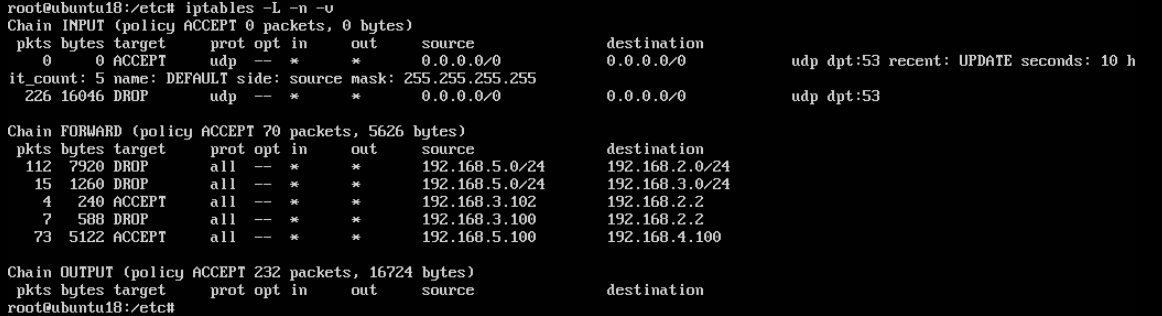
sudo iptables -A FORWARD -s 192.168.3.102 -d 192.168.2.2 -j ACCEPT

sudo iptables -A FORWARD -s 192.168.3.100 -d 192.168.2.2 -j DROP

sudo iptables -A FORWARD -s 192.168.5.100 -d 192.168.4.100 -j ACCEPT

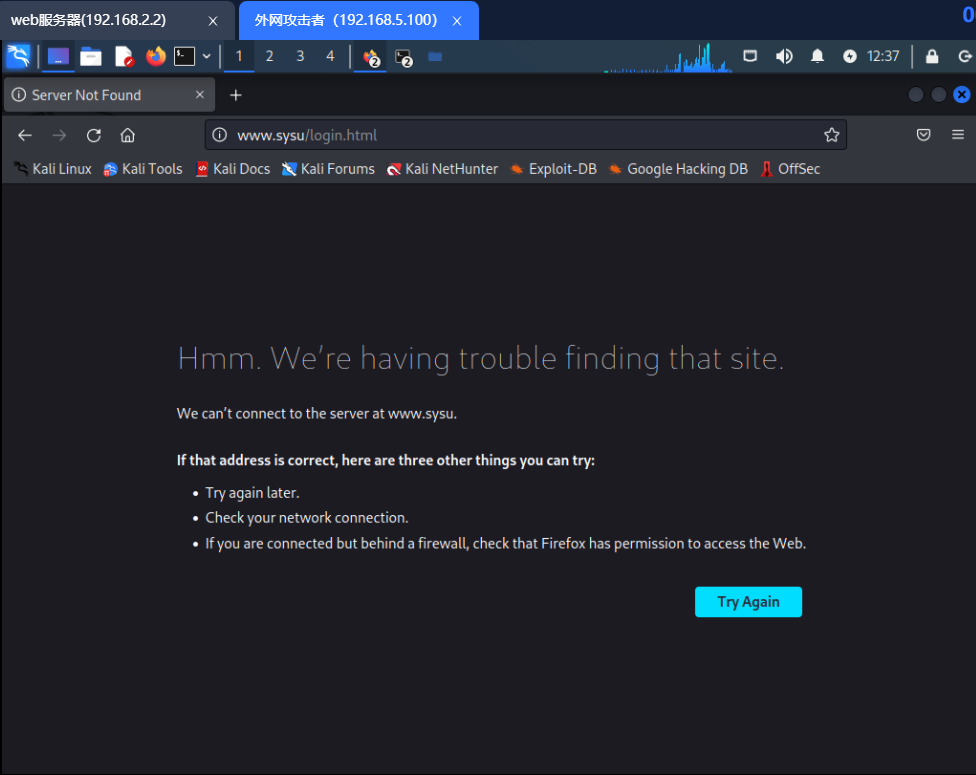
iptables -A INPUT -p udp --dport 53 -m recent --update --second 10 --hitcount 5 -j ACCEPT

iptables -A INPUT -p udp --dport 53 -j DROP

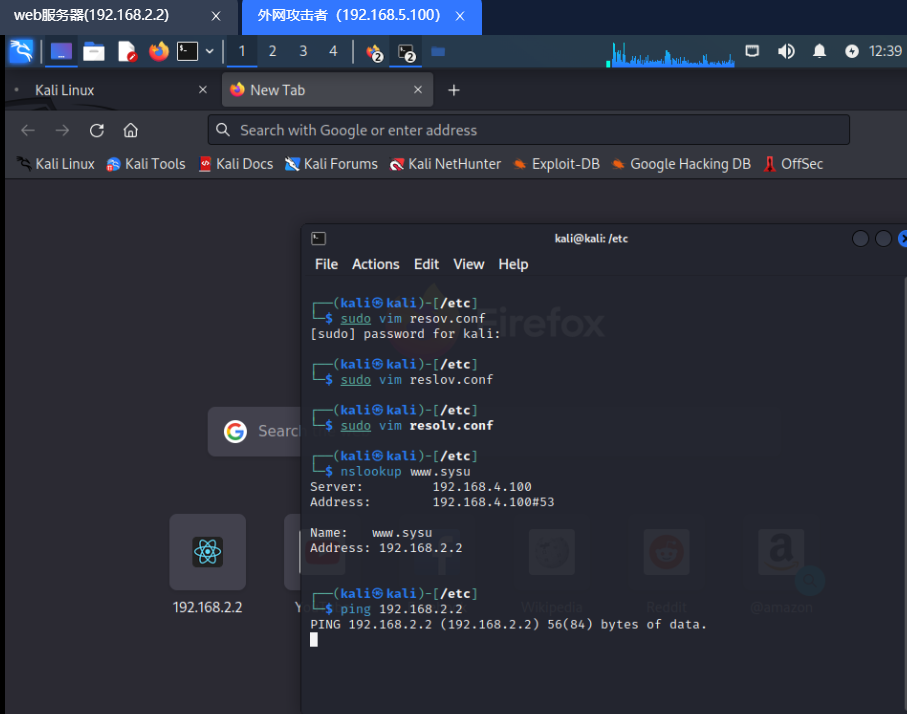


6、验证防火墙网关的有效性

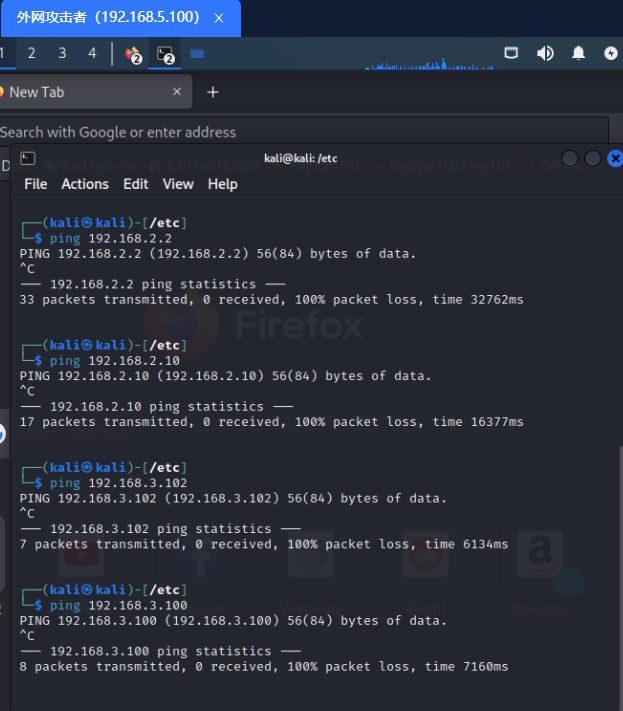
攻击者无法访问[www.sysu](http://www.sysu)



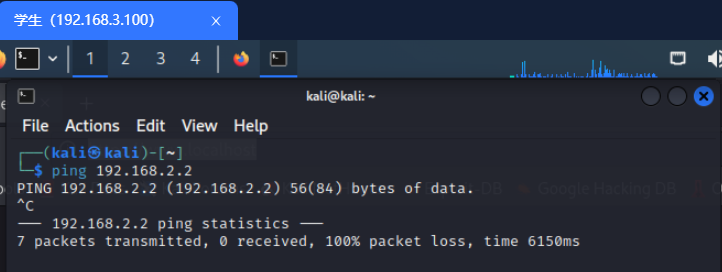
攻击者无法ping 192.168.2.2



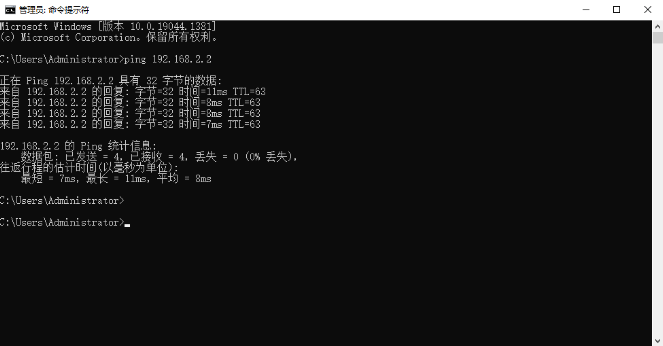
攻击者无法访问本地DNS，教师，学生。



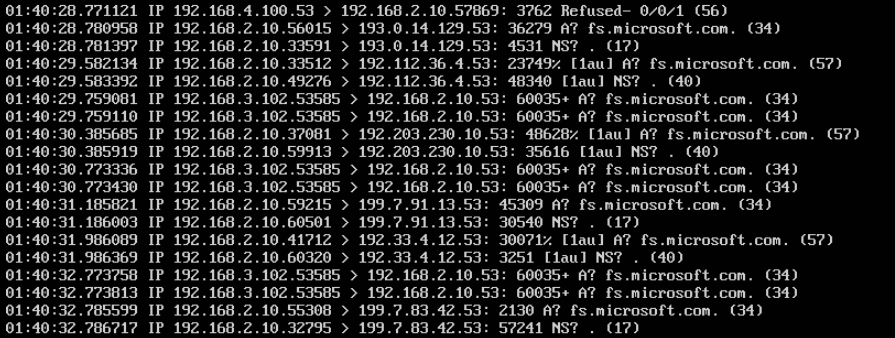
学生无法ping 192.168.2.2



教师无法ping 192.168.2.2



设置本地DNS请求限制速度不得超过5次/10秒之前



设置本地DNS请求限制速度不得超过5次/10秒之后

