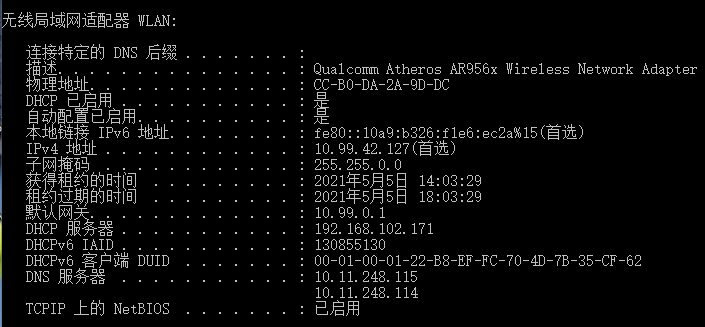
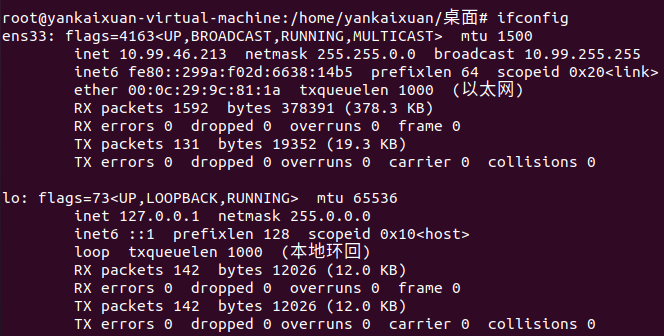
## 实验目的：本机通过arp攻击去攻击虚拟机使虚拟机无法上网

1. 通过ipconfig指令获取本机信息，通过ifconfig获取虚拟机信息





获取到的信息如下：

攻击者：

本机IP地址：10.99.42.127

本机MAC地址：CC:B0:DA:2A:9D:DC

受害者：

虚拟机IP地址：10.99.46.213

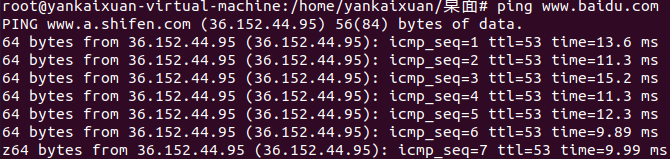
虚拟机MAC地址：00:0C:29:9C:81:1A

1. 请求攻击

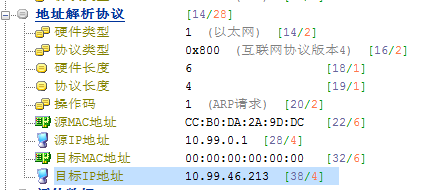
攻击前通过arp -a指令查看虚拟机（受害者）的arp缓存

3

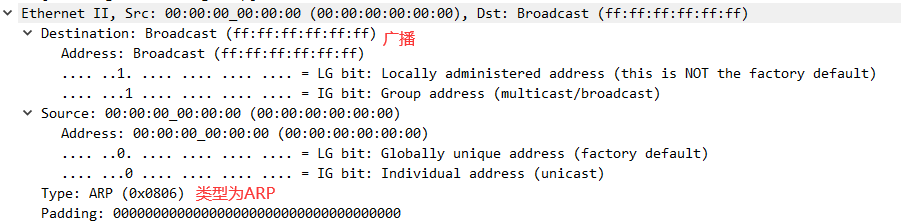
此时虚拟机可以上网

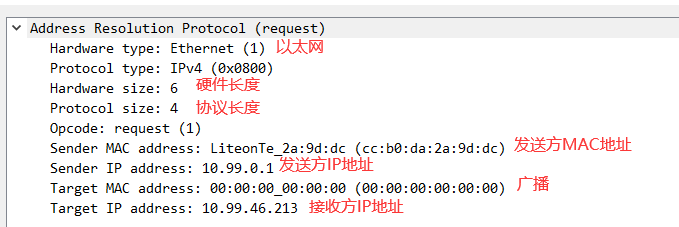


构造请求数据包



进行抓包，可以看到详细信息





查看虚拟机缓存，发现了变化，此时已经上不了网了。

}TD)~7R1GP6K2GMBU~BUNG0

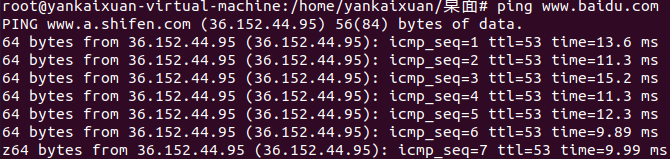
6

1. 响应攻击

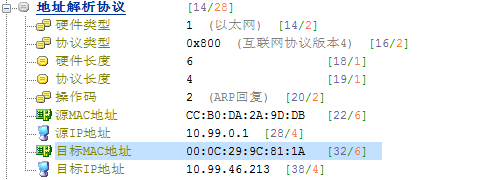
攻击前通过arp -a指令查看虚拟机（受害者）的arp缓存

3

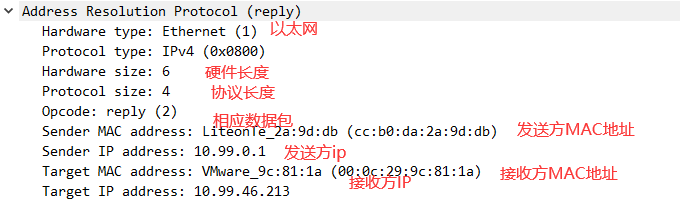
此时虚拟机可以上网



构造响应数据包：



进行抓包：



开始攻击，发现虚拟机已经上不了网了

6

查看缓存表

(6AHN8[%EB]PMN67J@I9KNQ

发现了变化，虚拟机网关物理地址变成了攻击者的物理地址。

1. 免费ARP

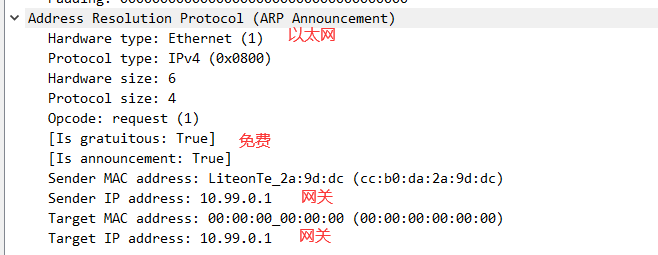
免费ARP是指主机发送ARP查找自己的IP地址。通常，它发生在系统引导期间进行接口配置的时候。目前免费ARP的作用有两种：

第一种：宣告广播的作用，告诉整个广播域，目前这个IP所对应的MAC地址是什么。

第二种：看广播域内有没有别的主机使用自己的IP，如果使用了，则在界面上弹出“IP冲突”字样。

免费ARP的报文发出去是不希望收到回应的，只希望是起宣告作用；如果收到回应，则证明对方也使用自己目前使用的IP地址。在所有网络设备（包括计 算机网卡）up的时候，都会发送这样的免费ARP广播，以宣告并确认有没有冲突。[1]

进行抓包



此时虚拟机无法上网。

1. ARP攻击的防范

对ARP攻击的防范很难做到，但仍有一些技术可以尽量做到防御：

1. 静态绑定网关MAC
2. ARP防火墙
3. VLAN和交换机端口绑定