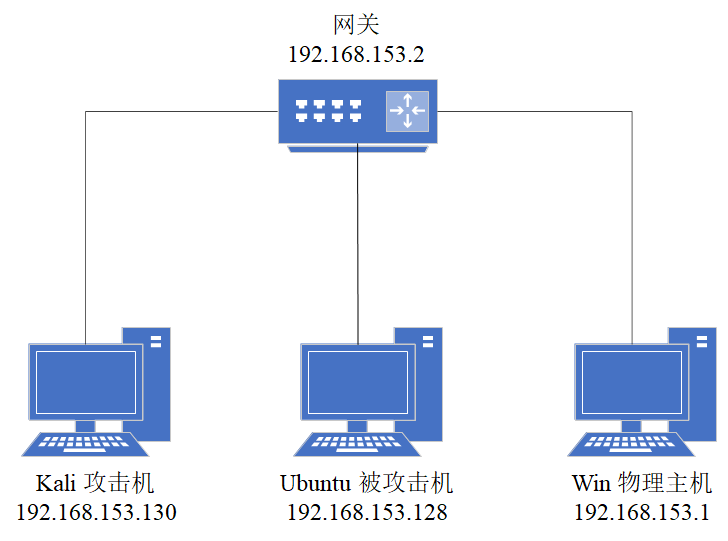
计算机网络第五次实验

姓名：黄瑞轩 学号：PB20111686

1. 实验环境搭建

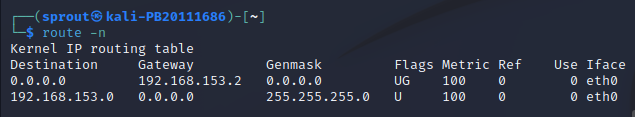
本次实验的网络拓扑图如下：

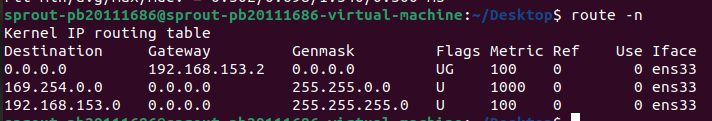


各主机的详细信息如下：

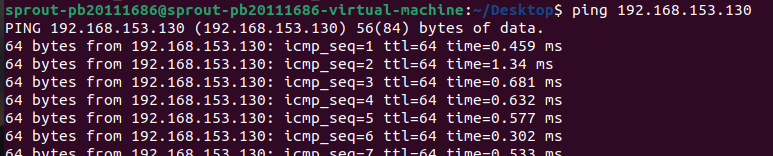
|  |  |  |
| --- | --- | --- |
| **主机** | **IP地址** | **操作系统版本** |
| Win物理主机 | 192.168.153.1 | Windows 10 |
| Ubuntu被攻击机 | 192.168.153.128 | Ubuntu 22.04 |
| Kali攻击机 | 192.168.153.130 | Kali 2022.4 |

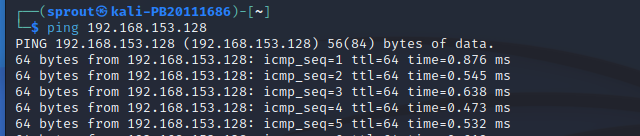
网关为192.168.153.2，获取截图如下：





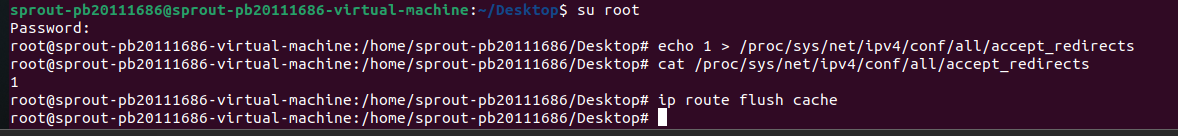
此时两台虚拟机之间可以互相ping通：





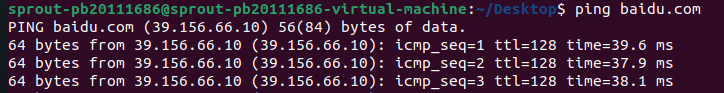
1. ICMP重定向攻击

首先按照PPT的提示，关闭一些系统已定义好的防护措施。

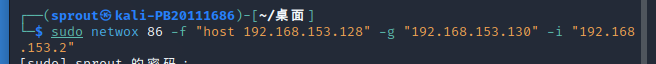


此时Ubuntu被攻击机可以访问百度，ping也正常：

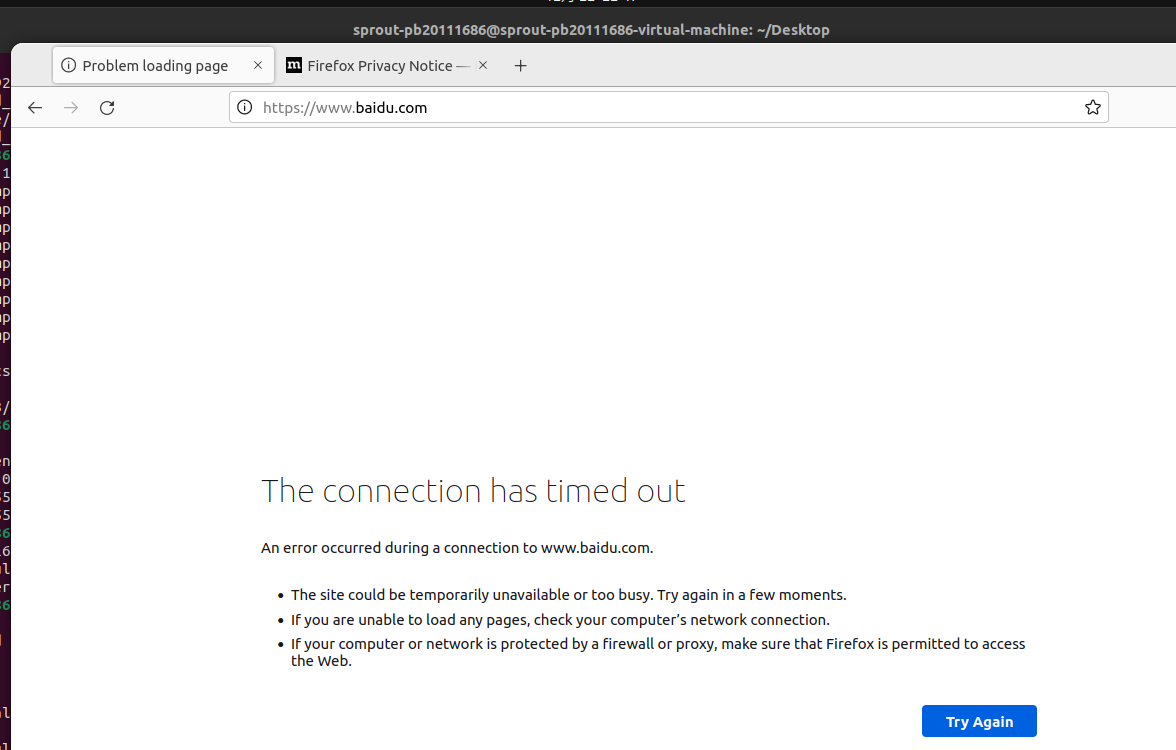


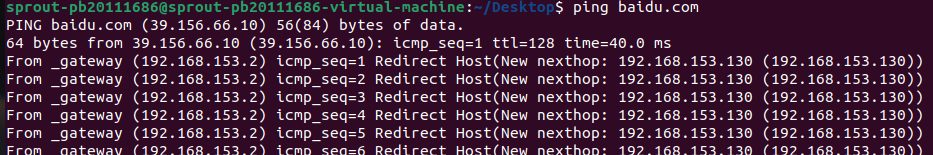


在Kali攻击机上安装Netwox，并发起ICMP重定向攻击：

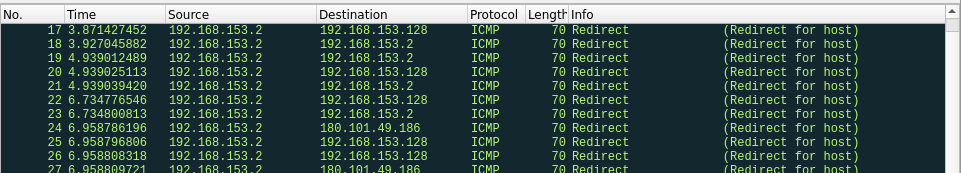


攻击成功，现在Ubuntu被攻击机不能访问百度了：





报文抓取结果：

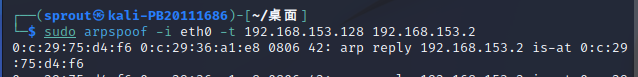


1. ARP断网攻击

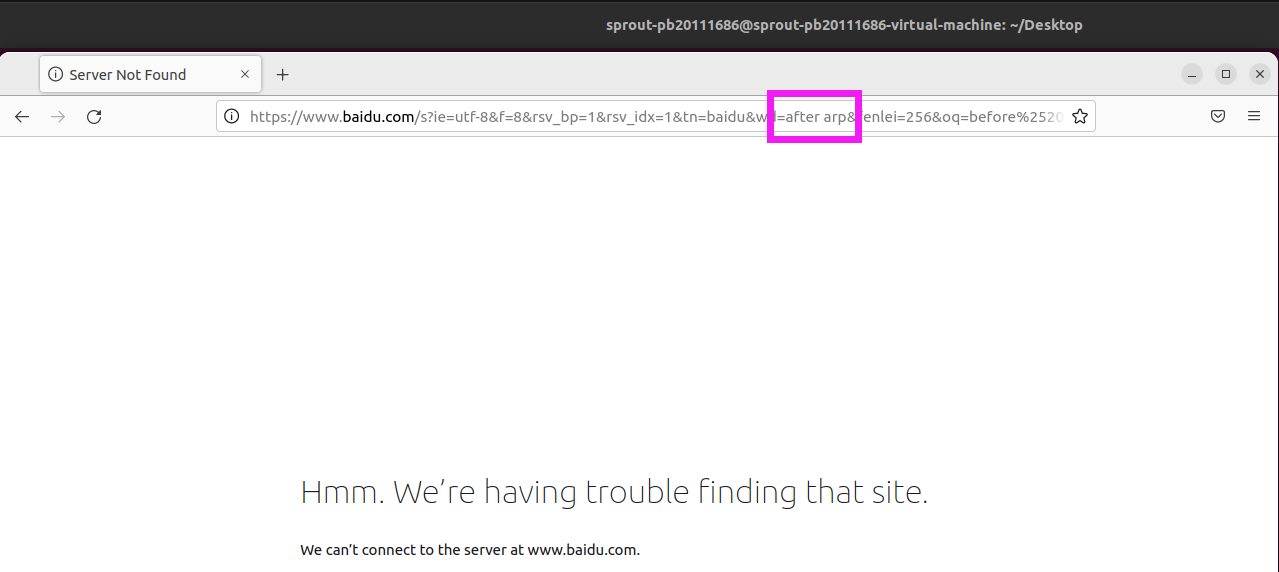
在攻击之前，Ubuntu被攻击机可以正常访问网页：



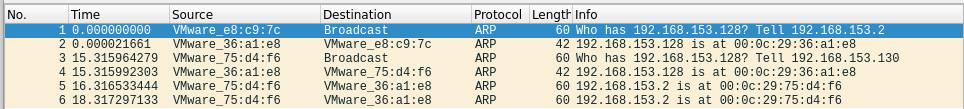
使用arpspoof命令攻击：



被攻击之后，Ubuntu被攻击机不能正常访问网页了：

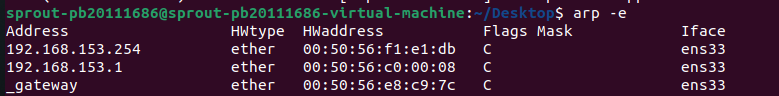


报文抓取结果：



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：



攻击后Ubuntu被攻击机ARP表：

