

**本科实验报告**

|  |  |
| --- | --- |
| 课程名称： | 网络安全原理与实践 |
| 姓 名： | 展翼飞 |
| 学 院： | 计算机科学与技术学院 |
| 系： | 计算机科学与技术系 |
| 专 业： | 计算机科学与技术 |
| 学 号： | 3190102196 |
| 指导教师： | 林峰 |

2024 年 3 月 21 日

**浙江大学实验报告**

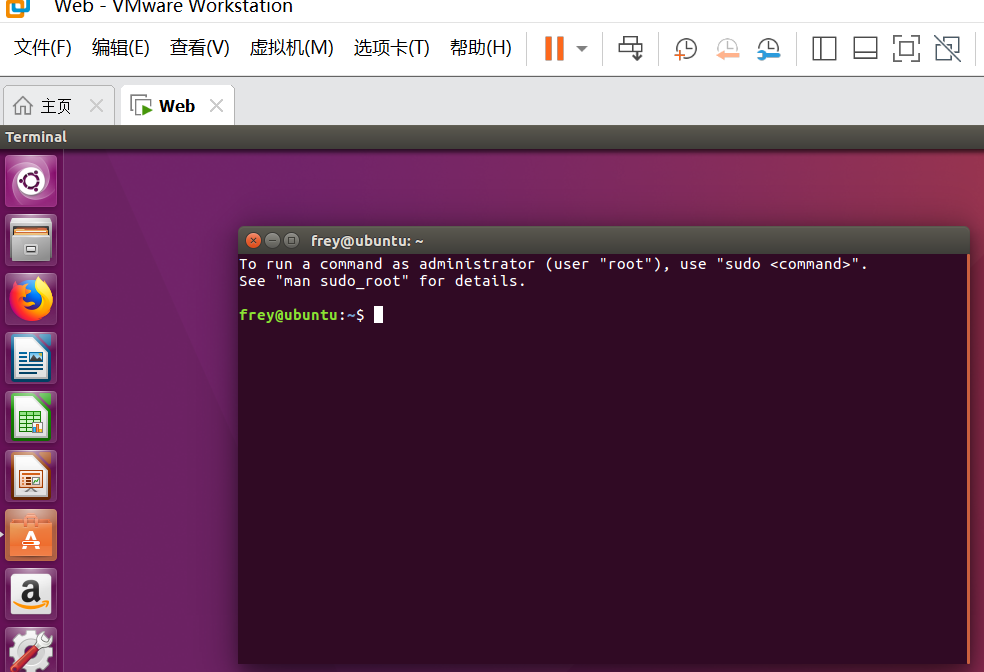
课程名称：网络安全原理与实践

实验名称：Lab 02

**LAB REQUIREMENTS:**

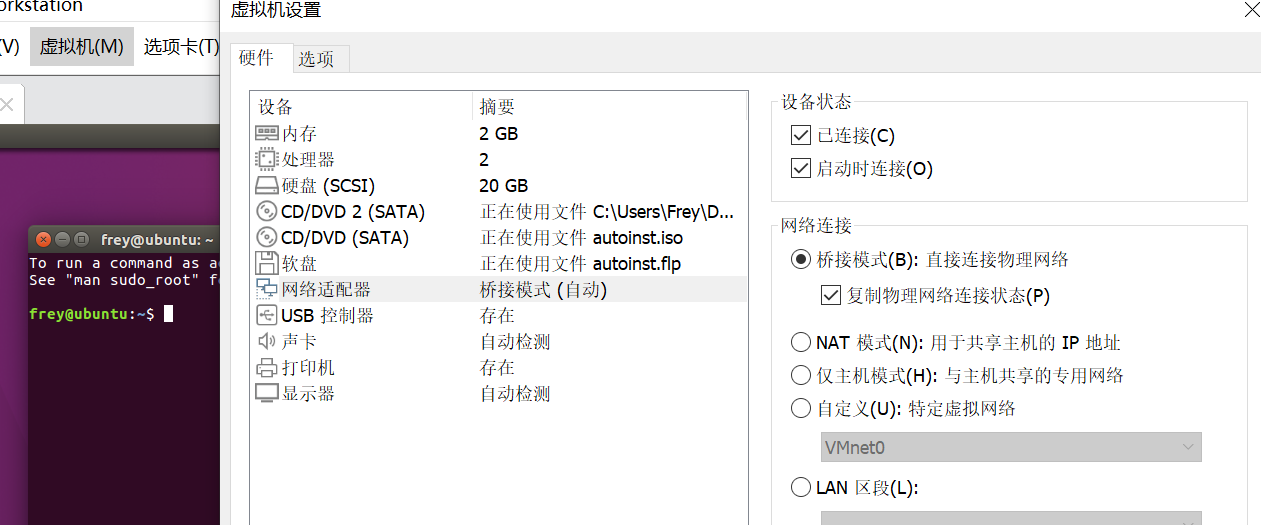
1. **Create a virtual machine**

Creating a virtual machine with VMware and ubuntu 16.04 image:



**2. Configure IP address of the virtual machine**

**step 1. set the network connection mode to bridge mode.**



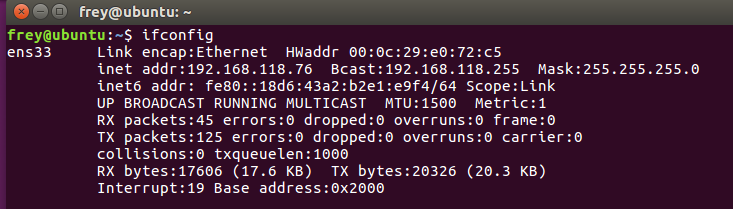
**step 2. modify the IP address and DNS address of the virtual machine to make**

**them in the same network segment as the host network.**

Switch the WLAN of host machine to hotspot of cellphone, shut down ipv6 and use command ipconfig to look up ip address of host:



Use ifconfig command to look up ip address of virtual machine to ensure them in the same network segment as host network:

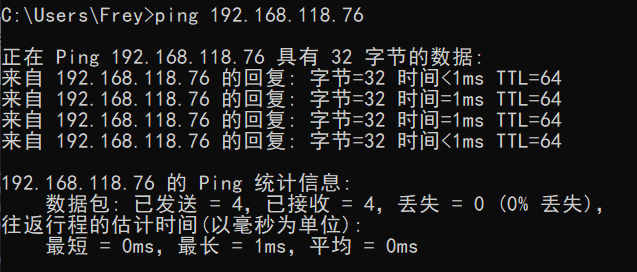


They are in the same segment.

**step 3. ensure that the virtual machine and the host can ping each other (note that you may need to turn off the host firewall; if you use wireless network, it is**

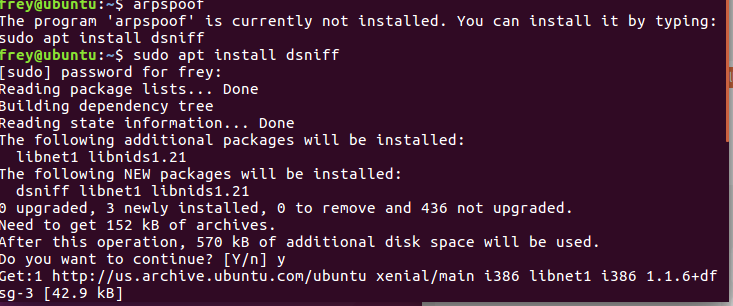
**recommended to turn on the hotspot; different behaviors may appear when using the ZJUWLAN.)**

Try to Ping virtual machine via host:



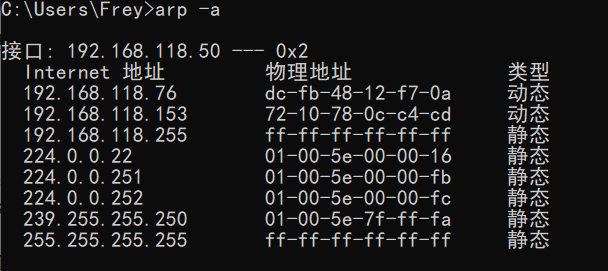
We can see that the host and the virtual machine are in the same net segment and can ping each other.

**step 4. install dsniff in the virtual machine**



**3. Start the ARP Spoofing**

**Step1. Enter ‘arp -a’ in the host computer to view the ARP cache.**

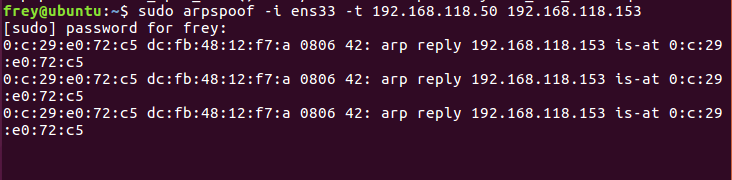


The physical address of gateway of host is 72-10-78-0c-c4-cd

**step 2. Run the instruction ‘sudo arpspoof -i [network card] -t [target IP] [host IP]’**

We use the follow command on the virtual machine to practice ARP spoofing toward the host:

arpspoof -i ens33 -t 192.168.118.50 192.168.118.153



**step 3. Surf the Internet on the host computer and observe the network status**

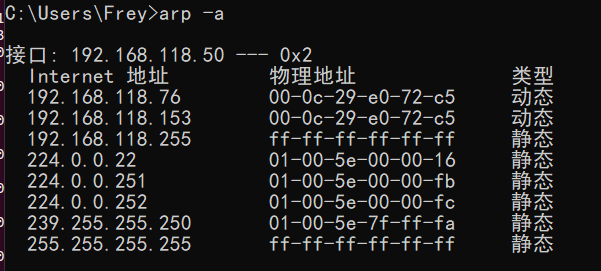


Because the MAC address of the gateway in the host’s ARP cache is changed by the ARP spoofing attack, the internet packet on the host can not be transfer to gateway, then the https request has no answer back to the host

**Step4. Enter ‘arp -a’ in the host computer to view the ARP cache. Compare the**

**gateway MAC address and the virtual machine MAC address.**

Enter arp -a in the host computer:



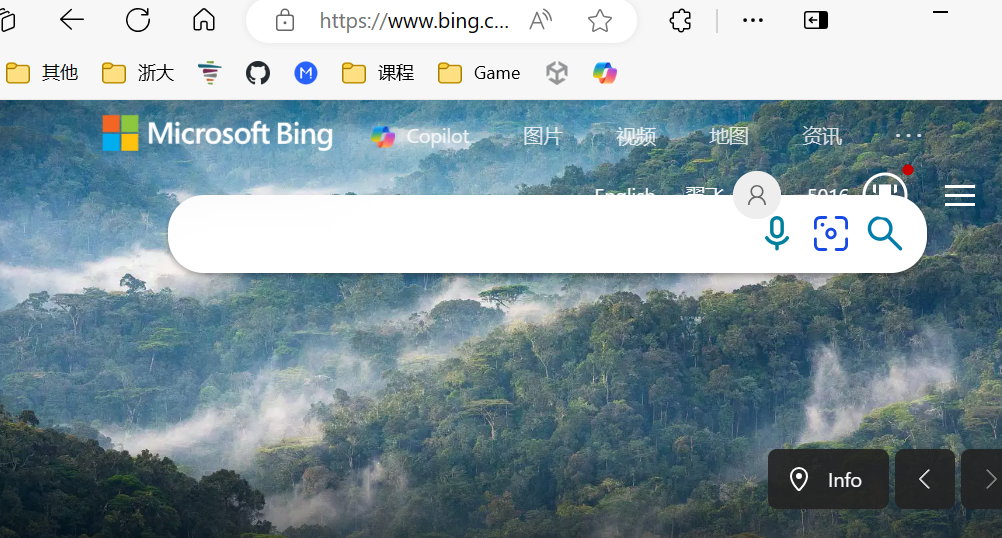
We can see that the gateway MAC address is the same with virtual machine MAC address

**Step5. Using ‘ctrl+c’ to interrupt the command in VM and check the host network status**

Interrupt the command in VM:



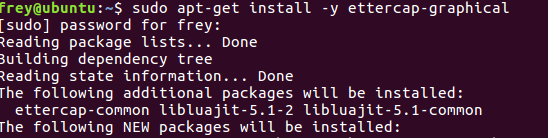
Check the host network status:



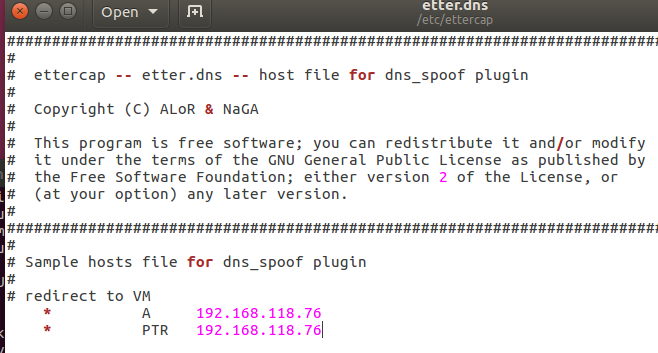
The network go back to normal.

**4. Start the DNS Spoofing**

**Step1. Install ettercap on the VM**

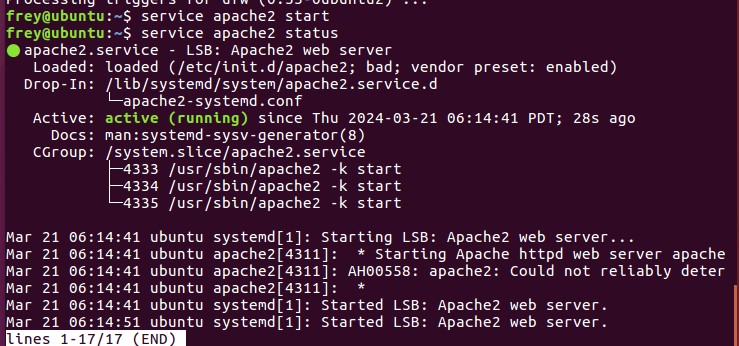


**Step2. Modify DNS file of ettercap on VM**



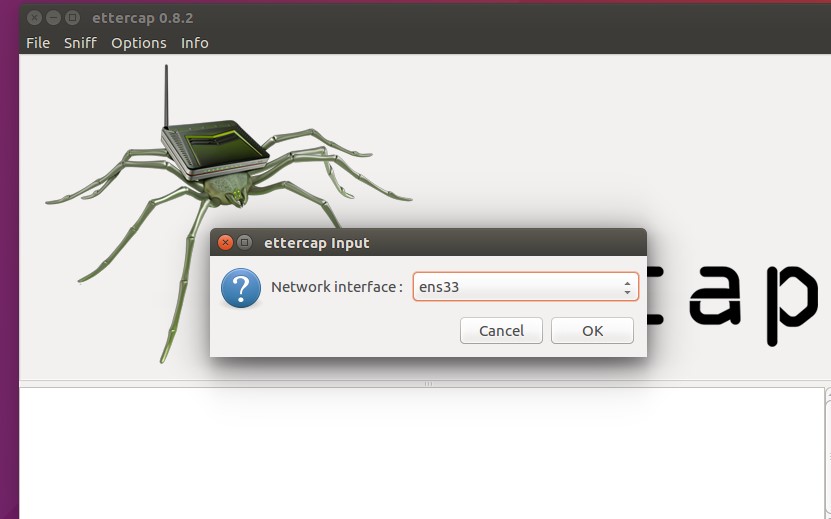
Add the content above in /etc/ettercap/etter.dns in VM to redirect any DNS query to the VM when the DNS spoofing happen

**Step3. Start apache on VM acting as malicious website**

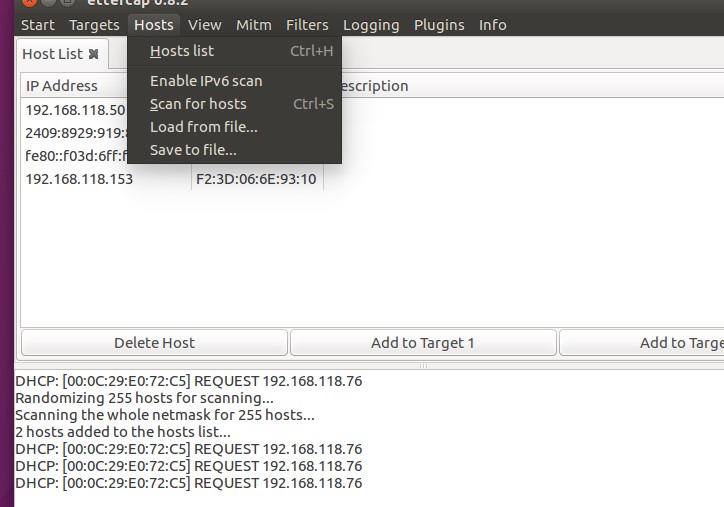
****

**Step 4. Open ettercap on VM**

Choose the net card and start sniffing

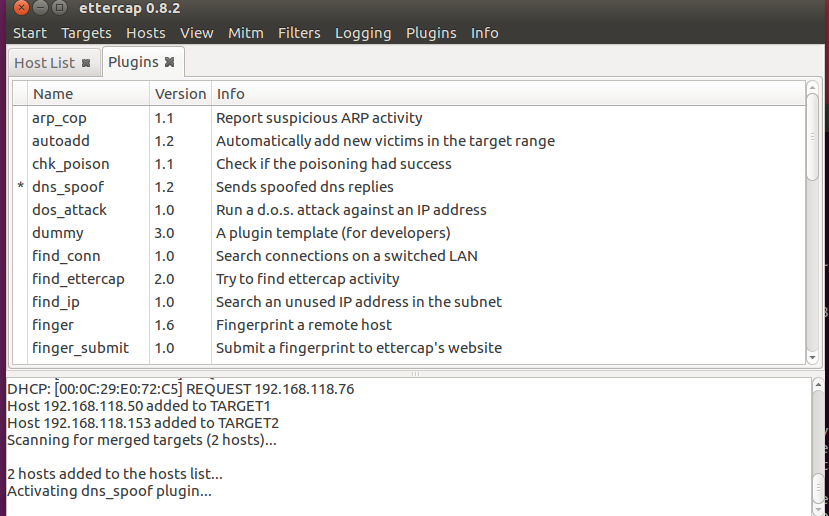
****

Scan for hosts and we can find gateway and host in the host list



Add the host to target1 and gateway to target 2, then start DNS spoofing in

Plugins –> manage plugins –> dns spoof



**Step 5. Test on the host**

Host’s opening website will be apache2(the malicious website set by VM) if it use domain name to query ip address.