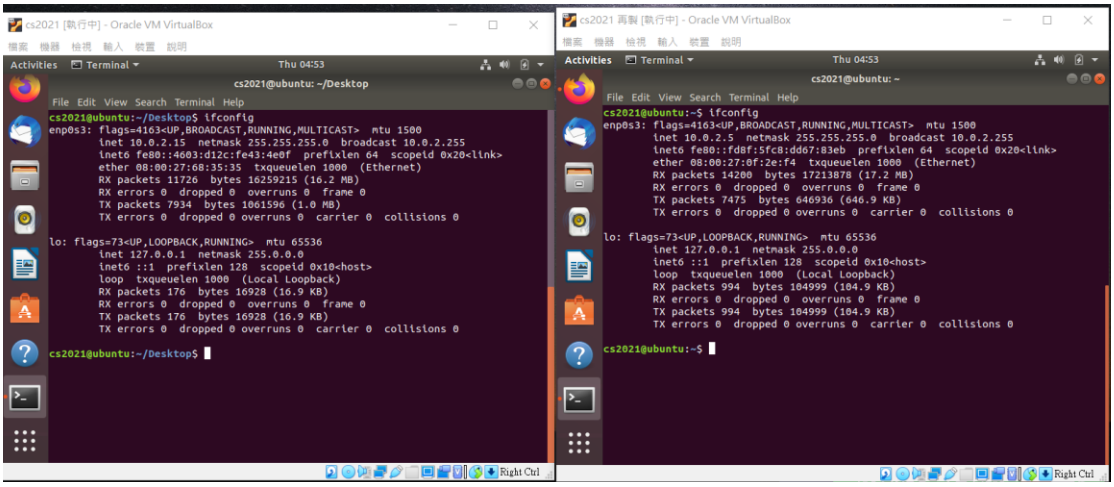
Computer Security HW2 Report

0716234 蕭彧

0713125 紀昀廷

Both of the attacks I use scenario two.

CIDR: 10.0.2.0/24
AP:10.0.2.1 MAC: 52:54:00:12:35:00
Attacker:10.0.2.15 MAC: 08:00:27:68:35:35
Victim:10.0.2.5 MAC: 08:00:27:0f:2e:f4


cs2021 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 04:53
cs2021@ubuntu: ~/Desktop
File Edit View Search Terminal Help
Right Ctrl
cs2021 再製 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 04:53
cs2021@ubuntu: ~
File Edit View Search Terminal Help
Right Ctrl

```
cs2021@ubuntu:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::4603:d12c:fe43:4e0f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:68:35:35  txqueuelen 1000  (Ethernet)
        RX packets 11726  bytes 16259215 (16.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7934  bytes 1061596 (1.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 176  bytes 16928 (16.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 176  bytes 16928 (16.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cs2021@ubuntu:~/Desktop$ 
```

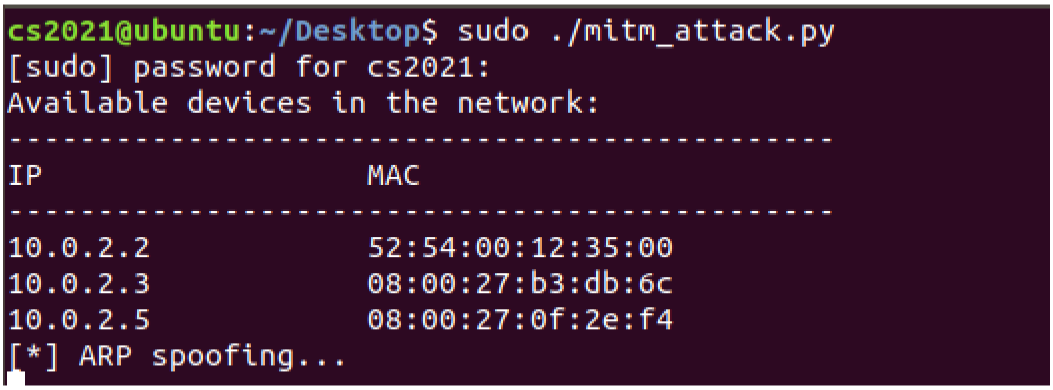
```
cs2021@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::fd8f:5fc8:dd67:83eb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0f:2e:f4  txqueuelen 1000  (Ethernet)
        RX packets 14200  bytes 17213878 (17.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7475  bytes 646936 (646.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 994  bytes 104999 (104.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 994  bytes 104999 (104.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cs2021@ubuntu:~$ 
```

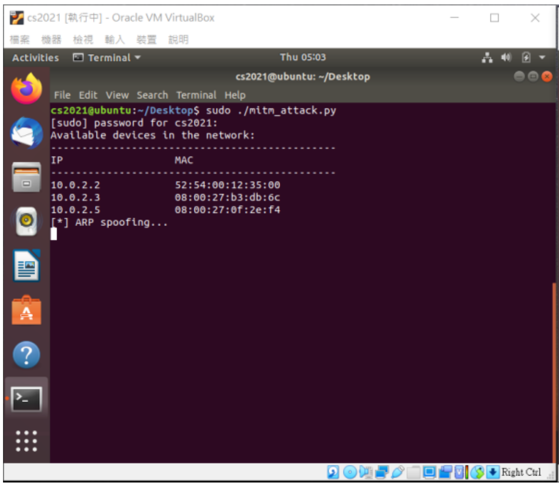
Part 1 MITM:

First, I scan all the wifi devices in network.

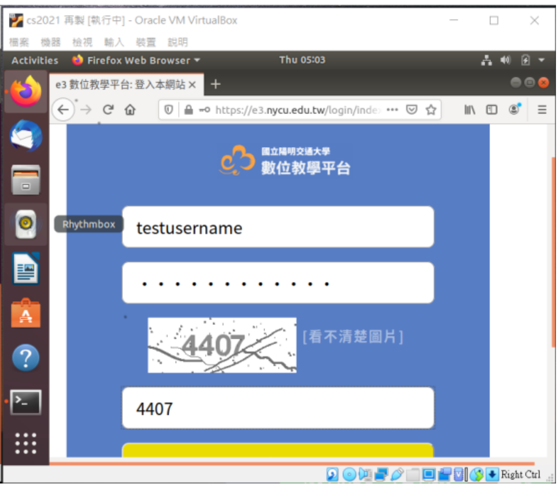


```
cs2021@ubuntu:~/Desktop$ sudo ./mitm_attack.py
[sudo] password for cs2021:
Available devices in the network:
---------------------------------------------
IP                  MAC
---------------------------------------------
10.0.2.2            52:54:00:12:35:00
10.0.2.3            08:00:27:b3:db:6c
10.0.2.5            08:00:27:0f:2e:f4
[*] ARP spoofing...
```

I input the username and password in victim’s website. The attacker then receives the input account information from victim.


cs2021 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 05:03
cs2021@ubuntu: ~/Desktop
File Edit View Search Terminal Help
Right Ctrl

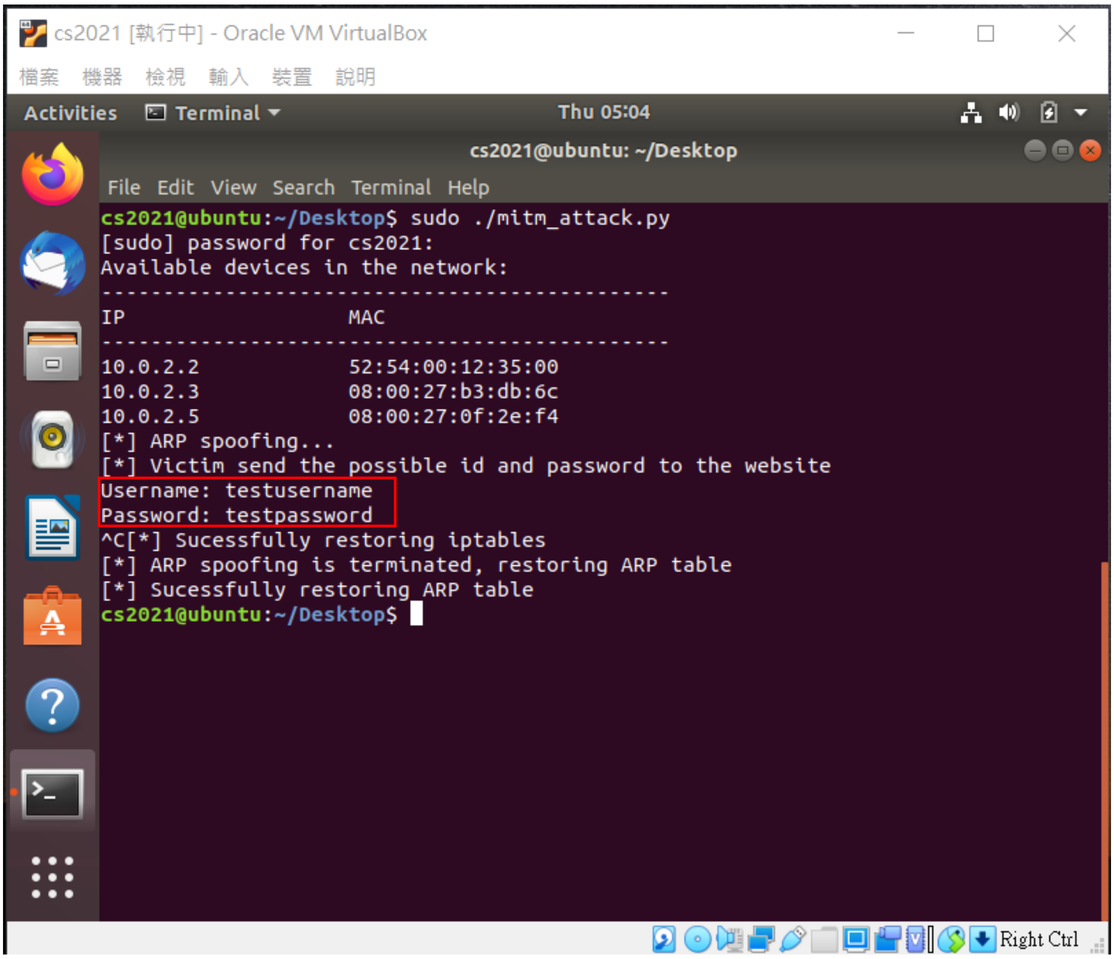
```
cs2021@ubuntu:~/Desktop$ sudo ./mitm_attack.py
[sudo] password for cs2021:
Available devices in the network:
---------------------------------------------
IP                  MAC
---------------------------------------------
10.0.2.2            52:54:00:12:35:00
10.0.2.3            08:00:27:b3:db:6c
10.0.2.5            08:00:27:0f:2e:f4
[*] ARP spoofing...
```


cs2021 再製 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Firefox Web Browser
Thu 05:03
e3 數位教學平台: 登入本網站
https://e3.nycu.edu.tw/login/inde
國立陽明交通大學
數位教學平台
Rhythmbox
[看不清楚圖片]
Right Ctrl

testusername

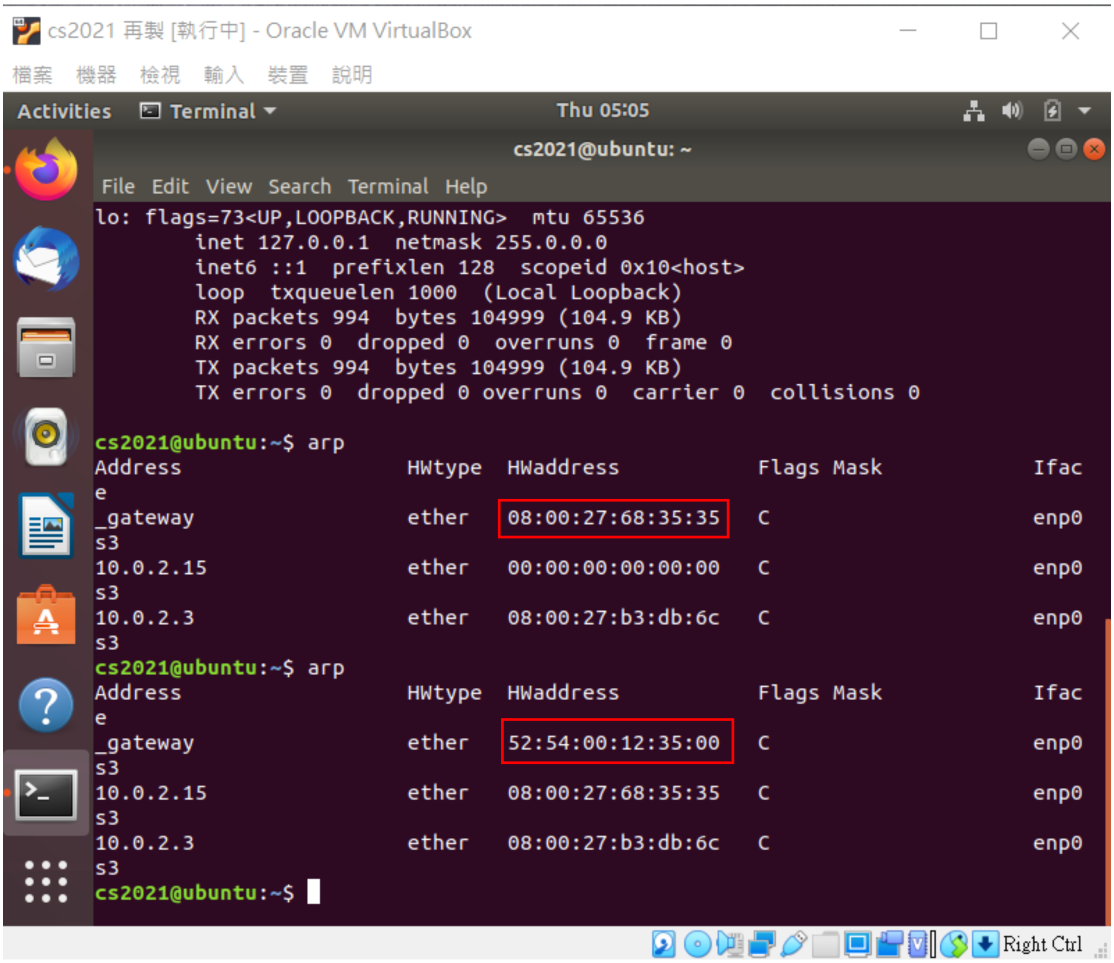
••••••••••••

4407


cs2021 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 05:04
cs2021@ubuntu: ~/Desktop
File Edit View Search Terminal Help
Right Ctrl

```
cs2021@ubuntu:~/Desktop$ sudo ./mitm_attack.py
[sudo] password for cs2021:
Available devices in the network:
---------------------------------------------
IP                  MAC
---------------------------------------------
10.0.2.2            52:54:00:12:35:00
10.0.2.3            08:00:27:b3:db:6c
10.0.2.5            08:00:27:0f:2e:f4
[*] ARP spoofing...
[*] Victim send the possible id and password to the website
Username: testusername
Password: testpassword
^C[*] Sucessfully restoring iptables
[*] ARP spoofing is terminated, restoring ARP table
[*] Sucessfully restoring ARP table
cs2021@ubuntu:~/Desktop$
```

In victim machine, we can see that the arp table change. From the gateway mac address has been spoofed to attacker's mac address to the correct mac address of gateway after the attack was over. It shows that our man in the middle attack is successful.

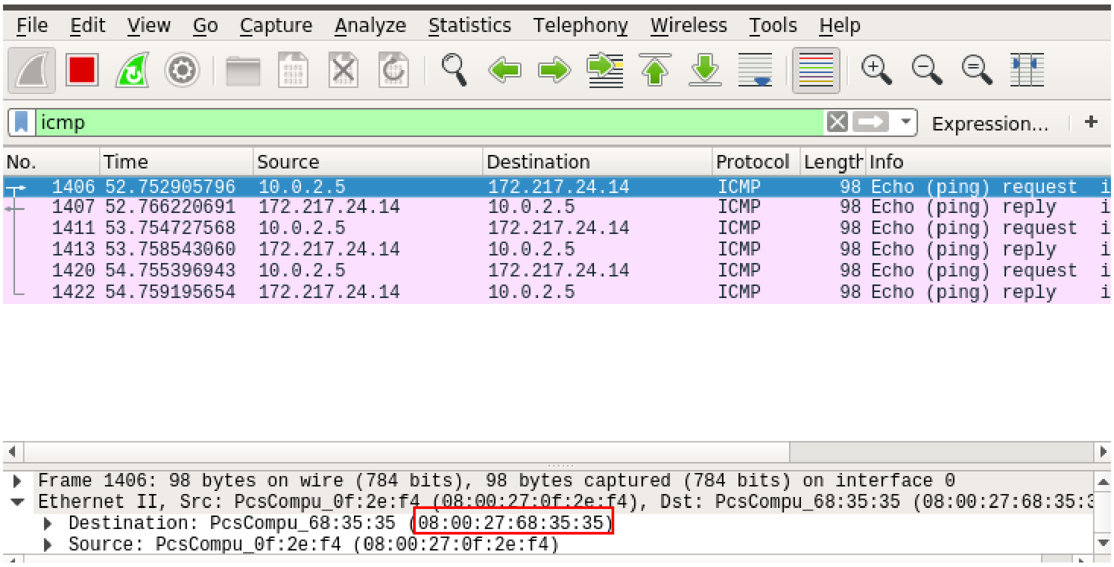


cs2021 再製 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 05:05
cs2021@ubuntu: ~
File Edit View Search Terminal Help
Right Ctrl

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 994  bytes 104999 (104.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 994  bytes 104999 (104.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cs2021@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   08:00:27:68:35:35   C                     enp0s3
10.0.2.15                ether   00:00:00:00:00:00   C                     enp0s3
10.0.2.3                 ether   08:00:27:b3:db:6c   C                     enp0s3
cs2021@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:00   C                     enp0s3
10.0.2.15                ether   08:00:27:68:35:35   C                     enp0s3
10.0.2.3                 ether   08:00:27:b3:db:6c   C                     enp0s3
cs2021@ubuntu:~$
```

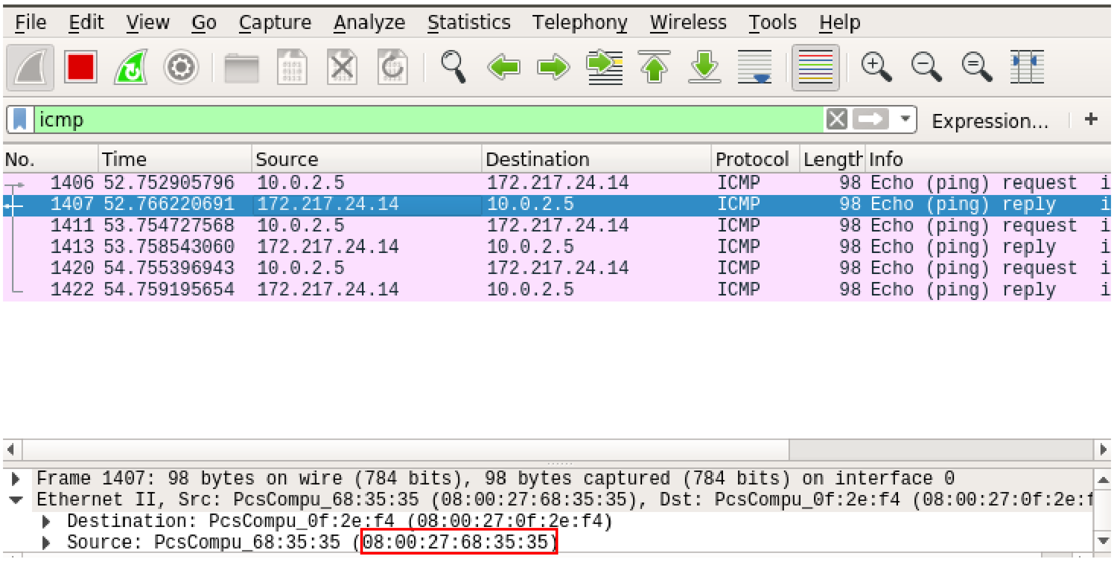
The following two picture also show that the packets all pass the attacker's machine, since the mac address of source and destination of the packets are attacker.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

Filter: icmp

```
No.   Time           Source         Destination    Protocol Length Info
 1406 52.752905796  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1407 52.766220691  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
 1411 53.754727568  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1413 53.758543060  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
 1420 54.755396943  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1422 54.759195654  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
```

```
▶ Frame 1406: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Ethernet II, Src: PcsCompu_0f:2e:f4 (08:00:27:0f:2e:f4), Dst: PcsCompu_68:35:35 (08:00:27:68:35:3
  ▶ Destination: PcsCompu_68:35:35 (08:00:27:68:35:35)
  ▶ Source: PcsCompu_0f:2e:f4 (08:00:27:0f:2e:f4)
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

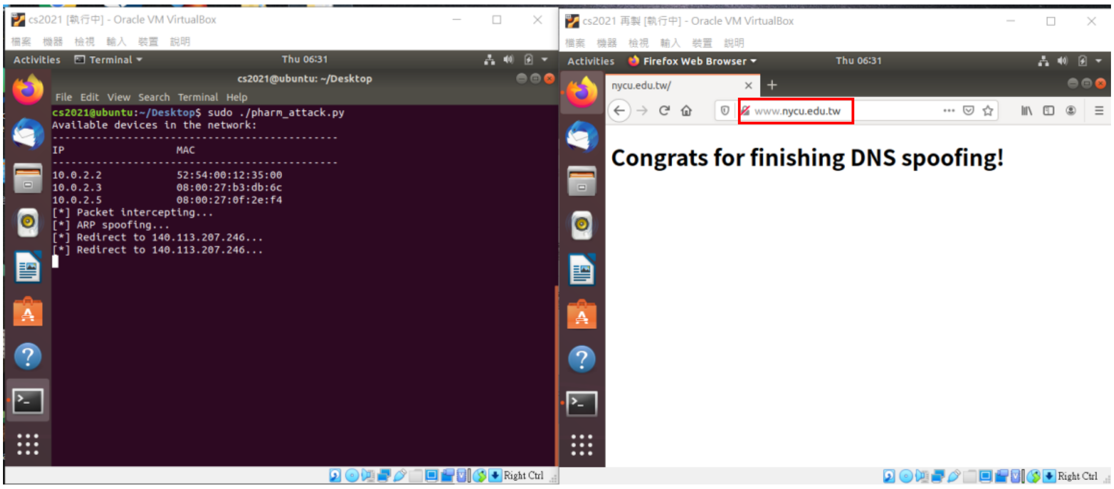
Filter: icmp

```
No.   Time           Source         Destination    Protocol Length Info
 1406 52.752905796  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1407 52.766220691  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
 1411 53.754727568  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1413 53.758543060  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
 1420 54.755396943  10.0.2.5       172.217.24.14  ICMP       98 Echo (ping) request  i
 1422 54.759195654  172.217.24.14  10.0.2.5       ICMP       98 Echo (ping) reply    i
```

```
▶ Frame 1407: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Ethernet II, Src: PcsCompu_68:35:35 (08:00:27:68:35:35), Dst: PcsCompu_0f:2e:f4 (08:00:27:0f:2e:f
  ▶ Destination: PcsCompu_0f:2e:f4 (08:00:27:0f:2e:f4)
  ▶ Source: PcsCompu_68:35:35 (08:00:27:68:35:35)
```

Part 2: Pharming attack

I launch the pharming attack in attacker’s machine. In the victim’s machine we can see that the www.nycu.edu.tw website shows the content of our spoofing web server, which shows the pharming attack success.

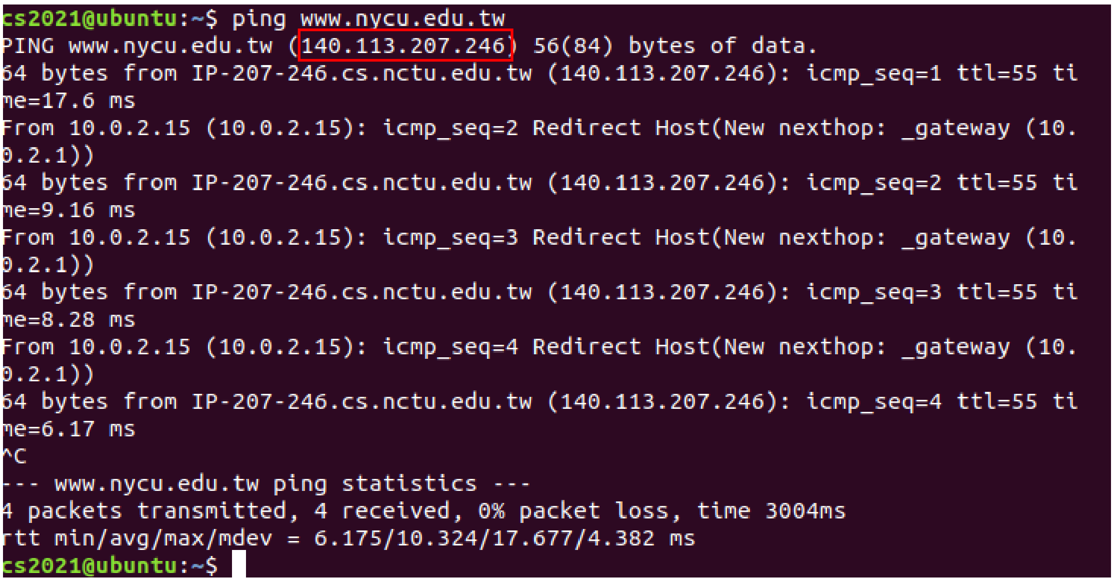


cs2021 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
Thu 06:31
cs2021@ubuntu: ~/Desktop
File Edit View Search Terminal Help
cs2021 再製 [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Firefox Web Browser
Thu 06:31
nycu.edu.tw/
www.nycu.edu.tw
Right Ctrl
Right Ctrl

```
cs2021@ubuntu:~/Desktop$ sudo ./pharm_attack.py
Available devices in the network:
----------------------------------------------
IP                  MAC
----------------------------------------------
10.0.2.2            52:54:00:12:35:00
10.0.2.3            08:00:27:b3:db:6c
10.0.2.5            08:00:27:0f:2e:f4
[*] Packet intercepting...
[*] ARP spoofing...
[*] Redirect to 140.113.207.246...
[*] Redirect to 140.113.207.246...
```

Congrats for finishing DNS spoofing!

We can also verify our pharmimg attack using ping. When I ping www.nycu.edu.tw, the ip of the website is our spoofed ip.



```
cs2021@ubuntu:~$ ping www.nycu.edu.tw
PING www.nycu.edu.tw (140.113.207.246) 56(84) bytes of data.
64 bytes from IP-207-246.cs.nctu.edu.tw (140.113.207.246): icmp_seq=1 ttl=55 ti
me=17.6 ms
From 10.0.2.15 (10.0.2.15): icmp_seq=2 Redirect Host(New nexthop: _gateway (10.
0.2.1))
64 bytes from IP-207-246.cs.nctu.edu.tw (140.113.207.246): icmp_seq=2 ttl=55 ti
me=9.16 ms
From 10.0.2.15 (10.0.2.15): icmp_seq=3 Redirect Host(New nexthop: _gateway (10.
0.2.1))
64 bytes from IP-207-246.cs.nctu.edu.tw (140.113.207.246): icmp_seq=3 ttl=55 ti
me=8.28 ms
From 10.0.2.15 (10.0.2.15): icmp_seq=4 Redirect Host(New nexthop: _gateway (10.
0.2.1))
64 bytes from IP-207-246.cs.nctu.edu.tw (140.113.207.246): icmp_seq=4 ttl=55 ti
me=6.17 ms
^C
--- www.nycu.edu.tw ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 6.175/10.324/17.677/4.382 ms
cs2021@ubuntu:~$ 
```

Part 3: Solution to defend against ARP spoofing attack

If the network is small, the ideal way to defend against ARP spoofing is using static ARP entries. Network devices can record the MAC address of all devices in the network by DHCP. Thus, we can detect ARP spoofing attack when receiving an ARP spoofing packet. Another way to prevent ARP spoofing from happening in the first place is to rely on Virtual Private Networks (VPNs). When you connect to the internet, you typically first connect to an Internet Service Provider (ISP) in order to connect to another website. However, when you use a VPN, you're using an encrypted tunnel that largely blocks your activity from ARP spoofing hackers. Both the method by which you're conducting the online activity and the data that goes through it is encrypted.