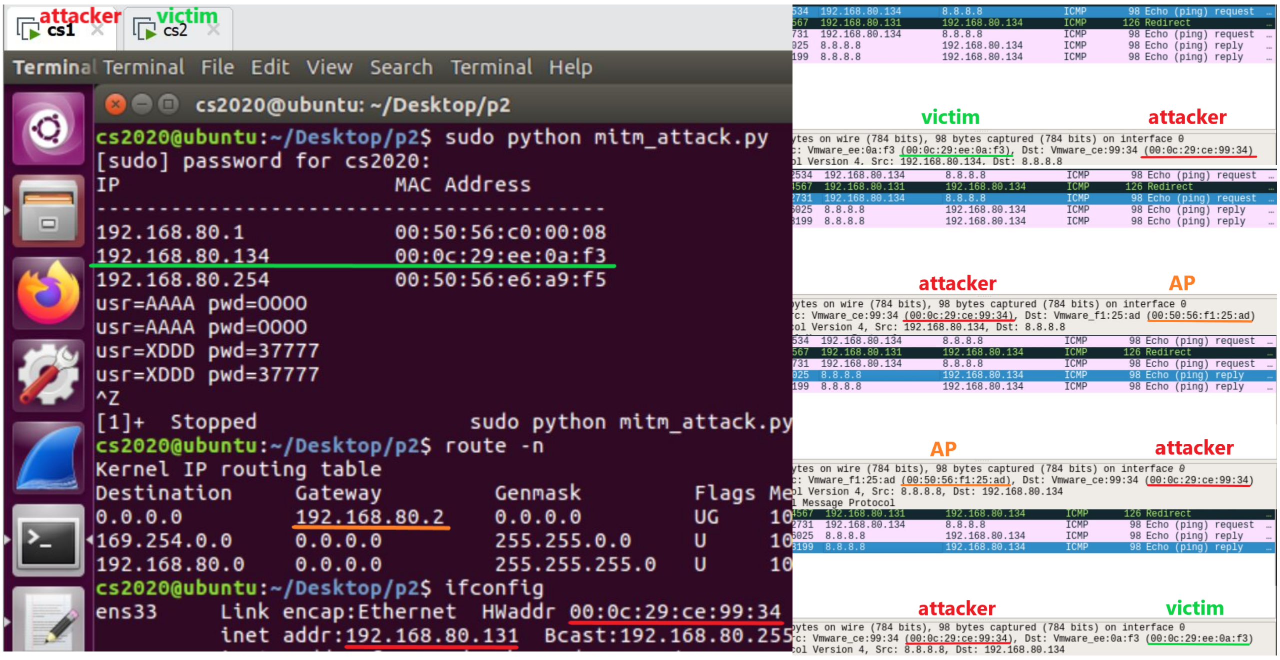
一


attacker
cs1
victim
cs2
Terminal
Terminal File Edit View Search Terminal Help
cs2020@ubuntu: ~/Desktop/p2

```
cs2020@ubuntu:~/Desktop/p2$ sudo python mitm_attack.py
[sudo] password for cs2020:
IP                       MAC Address
-----------------------------------------
192.168.80.1             00:50:56:c0:00:08
192.168.80.134           00:0c:29:ee:0a:f3
192.168.80.254           00:50:56:e6:a9:f5
usr=AAAA pwd=0000
usr=AAAA pwd=0000
usr=XDDD pwd=37777
usr=XDDD pwd=37777
^Z
[1]+  Stopped                 sudo python mitm_attack.py
cs2020@ubuntu:~/Desktop/p2$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Me
0.0.0.0         192.168.80.2    0.0.0.0         UG    10
169.254.0.0     0.0.0.0         255.255.0.0     U     10
192.168.80.0    0.0.0.0         255.255.255.0   U     10
cs2020@ubuntu:~/Desktop/p2$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:ce:99:34
          inet addr:192.168.80.131  Bcast:192.168.80.255
```

```
534  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
567  192.168.80.131   192.168.80.134   ICMP   126 Redirect             …
731  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
025  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
199  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
```

```
ytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
c: Vmware_ee:0a:f3 (00:0c:29:ee:0a:f3), Dst: Vmware_ce:99:34 (00:0c:29:ce:99:34)
ol Version 4, Src: 192.168.80.134, Dst: 8.8.8.8
2534  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
4567  192.168.80.131   192.168.80.134   ICMP   126 Redirect             …
2731  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
6025  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
8199  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
```

```
bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
rc: Vmware_ce:99:34 (00:0c:29:ce:99:34), Dst: Vmware_f1:25:ad (00:50:56:f1:25:ad)
col Version 4, Src: 192.168.80.134, Dst: 8.8.8.8
534  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
567  192.168.80.131   192.168.80.134   ICMP   126 Redirect             …
731  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
025  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
199  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
```

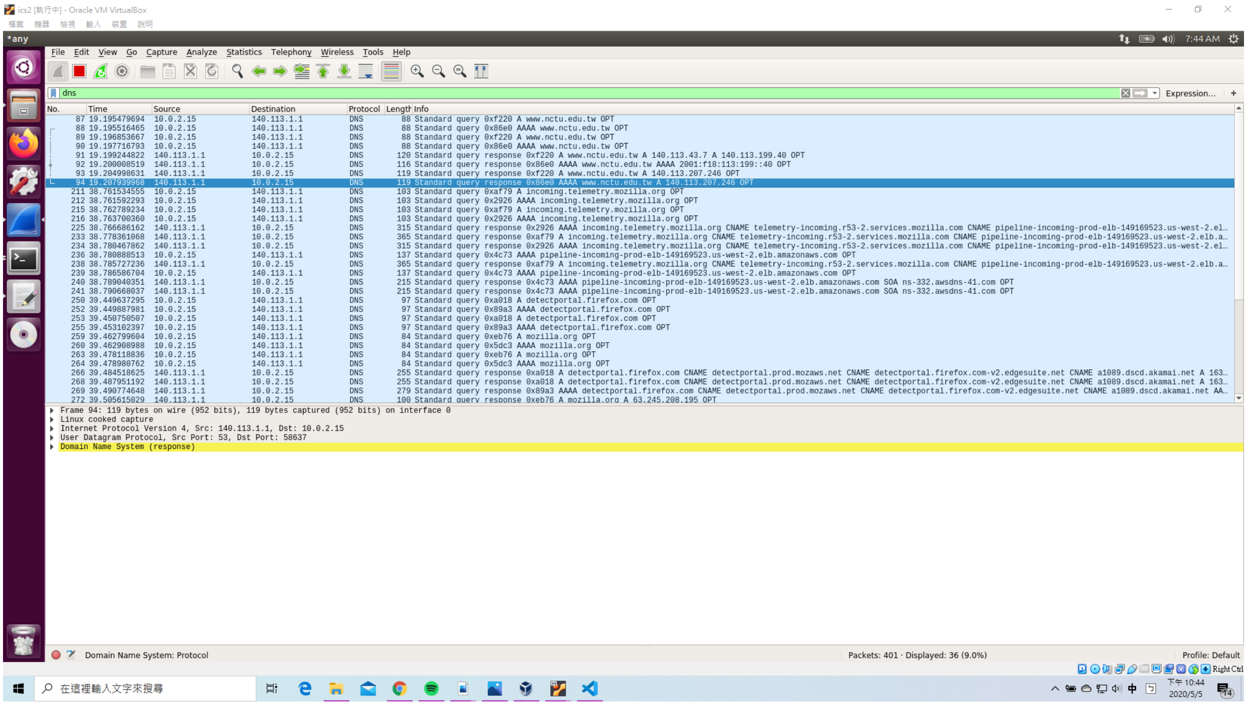
```
ytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
c: Vmware_f1:25:ad (00:50:56:f1:25:ad), Dst: Vmware_ce:99:34 (00:0c:29:ce:99:34)
ol Version 4, Src: 8.8.8.8, Dst: 192.168.80.134
l Message Protocol
4567  192.168.80.131   192.168.80.134   ICMP   126 Redirect             …
2731  192.168.80.134   8.8.8.8          ICMP    98 Echo (ping) request  …
6025  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
8199  8.8.8.8          192.168.80.134   ICMP    98 Echo (ping) reply    …
```

```
bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
rc: Vmware_ce:99:34 (00:0c:29:ce:99:34), Dst: Vmware_ee:0a:f3 (00:0c:29:ee:0a:f3)
col Version 4, Src: 8.8.8.8, Dst: 192.168.80.134
```

Firstly, get IP/MAC addresses of devices by sending ARP request across our LAN.
Next, send ARP packets with spoofed IP to gateway and victims.
(To tell the gateway that we are victim and tell the victims that we are gateway)
Lastly, sniff and fetch packets coming from victims, and print out the retrieved data.

ping 8.8.8.8 on victim VM after executing mitm_attack.py, serving as an example trace of arp spoofing

二



ics2 [執行中] - Oracle VM VirtualBox

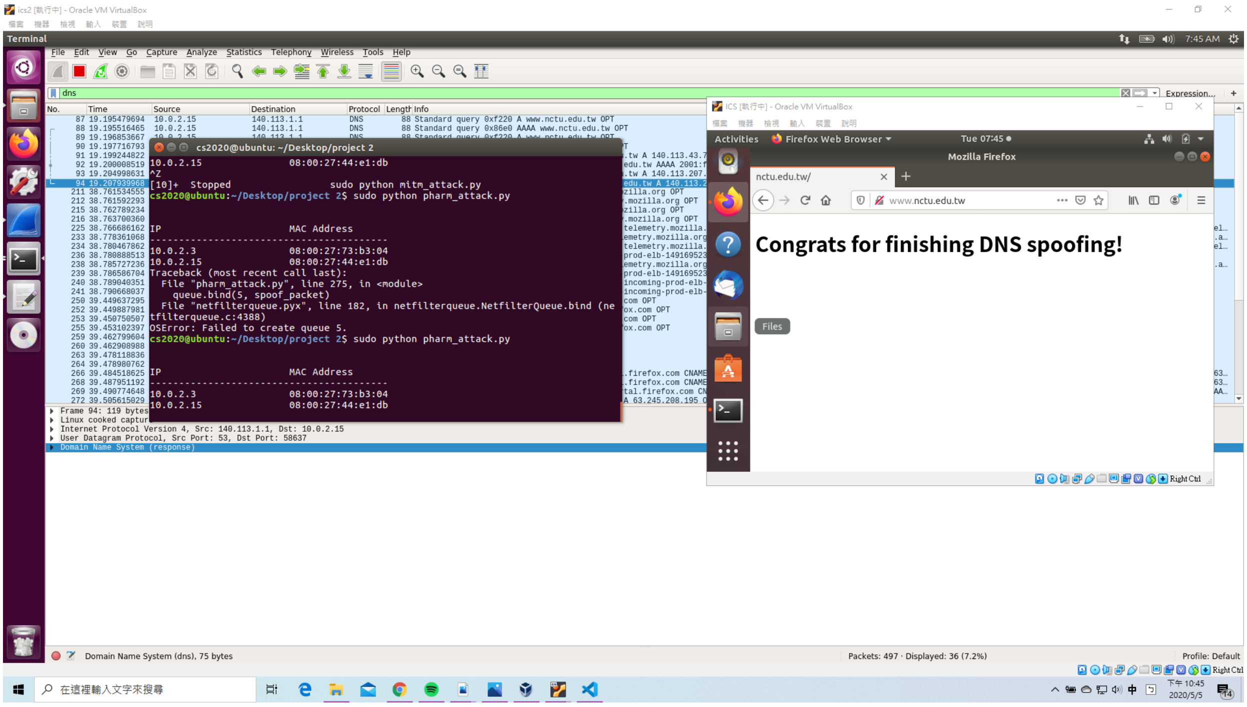
檔案 機器 檢視 輸入 裝置 說明
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…

```
No.  Time          Source        Destination   Protocol Length Info
  87 19.195479694  10.0.2.15     140.113.1.1   DNS      88  Standard query 0xf220 A www.nctu.edu.tw OPT
  88 19.195516465  10.0.2.15     140.113.1.1   DNS      88  Standard query 0x86e0 AAAA www.nctu.edu.tw OPT
  89 19.196853667  10.0.2.15     140.113.1.1   DNS      88  Standard query 0xf220 A www.nctu.edu.tw OPT
  90 19.197716793  10.0.2.15     140.113.1.1   DNS      88  Standard query 0x86e0 AAAA www.nctu.edu.tw OPT
  91 19.199244822  140.113.1.1   10.0.2.15     DNS      120 Standard query response 0xf220 A www.nctu.edu.tw A 140.113.43.7 A 140.113.199.40 OPT
  92 19.200008519  140.113.1.1   10.0.2.15     DNS      116 Standard query response 0x86e0 AAAA www.nctu.edu.tw AAAA 2001:f18:113:199::40 OPT
  93 19.204998631  140.113.1.1   10.0.2.15     DNS      119 Standard query response 0xf220 A www.nctu.edu.tw A 140.113.207.246 OPT
  94 19.207939968  140.113.1.1   10.0.2.15     DNS      119 Standard query response 0x86e0 AAAA www.nctu.edu.tw A 140.113.207.246 OPT
 211 38.761534555  10.0.2.15     140.113.1.1   DNS      103 Standard query 0xaf79 A incoming.telemetry.mozilla.org OPT
 212 38.761592293  10.0.2.15     140.113.1.1   DNS      103 Standard query 0x2926 AAAA incoming.telemetry.mozilla.org OPT
 215 38.762789234  10.0.2.15     140.113.1.1   DNS      103 Standard query 0xaf79 A incoming.telemetry.mozilla.org OPT
 216 38.763700360  10.0.2.15     140.113.1.1   DNS      103 Standard query 0x2926 AAAA incoming.telemetry.mozilla.org OPT
 225 38.766686162  140.113.1.1   10.0.2.15     DNS      315 Standard query response 0x2926 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com CNAME pipeline-incoming-prod-elb-149169523.us-west-2.el…
 233 38.778361068  140.113.1.1   10.0.2.15     DNS      365 Standard query response 0xaf79 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com CNAME pipeline-incoming-prod-elb-149169523.us-west-2.elb.a…
 234 38.780467862  140.113.1.1   10.0.2.15     DNS      315 Standard query response 0x2926 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com CNAME pipeline-incoming-prod-elb-149169523.us-west-2.el…
 236 38.780888513  10.0.2.15     140.113.1.1   DNS      137 Standard query 0x4c73 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com OPT
 238 38.785727236  140.113.1.1   10.0.2.15     DNS      365 Standard query response 0xaf79 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com CNAME pipeline-incoming-prod-elb-149169523.us-west-2.elb.a…
 239 38.786586704  10.0.2.15     140.113.1.1   DNS      137 Standard query 0x4c73 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com OPT
 240 38.789040351  140.113.1.1   10.0.2.15     DNS      215 Standard query response 0x4c73 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-41.com OPT
 241 38.790668037  140.113.1.1   10.0.2.15     DNS      215 Standard query response 0x4c73 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-41.com OPT
 250 39.449637295  10.0.2.15     140.113.1.1   DNS      97  Standard query 0xa018 A detectportal.firefox.com OPT
 252 39.449887981  10.0.2.15     140.113.1.1   DNS      97  Standard query 0x89a3 AAAA detectportal.firefox.com OPT
 253 39.450750507  10.0.2.15     140.113.1.1   DNS      97  Standard query 0xa018 A detectportal.firefox.com OPT
 255 39.453102397  10.0.2.15     140.113.1.1   DNS      97  Standard query 0x89a3 AAAA detectportal.firefox.com OPT
 259 39.462799604  10.0.2.15     140.113.1.1   DNS      84  Standard query 0xeb76 A mozilla.org OPT
 260 39.462908988  10.0.2.15     140.113.1.1   DNS      84  Standard query 0x5dc3 AAAA mozilla.org OPT
 263 39.478118836  10.0.2.15     140.113.1.1   DNS      84  Standard query 0xeb76 A mozilla.org OPT
 264 39.478980762  10.0.2.15     140.113.1.1   DNS      84  Standard query 0x5dc3 AAAA mozilla.org OPT
 266 39.484518625  140.113.1.1   10.0.2.15     DNS      255 Standard query response 0xa018 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.com-v2.edgesuite.net CNAME a1089.dscd.akamai.net A 163…
 268 39.487951192  140.113.1.1   10.0.2.15     DNS      255 Standard query response 0xa018 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.com-v2.edgesuite.net CNAME a1089.dscd.akamai.net A 163…
 269 39.490774648  140.113.1.1   10.0.2.15     DNS      279 Standard query response 0x89a3 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.com-v2.edgesuite.net CNAME a1089.dscd.akamai.net AA…
 272 39.505615029  140.113.1.1   10.0.2.15     DNS      100 Standard query response 0xeb76 A mozilla.org A 63.245.208.195 OPT

▸ Frame 94: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 140.113.1.1, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 58637
▸ Domain Name System (response)
```

Domain Name System: Protocol   Packets: 401 · Displayed: 36 (9.0%)   Profile: Default

7:44 AM
在這裡輸入文字來搜尋
下午 10:44
2020/5/5



ics2 [執行中] - Oracle VM VirtualBox

Terminal
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…
7:45 AM

cs2020@ubuntu: ~/Desktop/project 2

```
10.0.2.15                08:00:27:44:e1:db
^Z
[10]+  Stopped                 sudo python mitm_attack.py
cs2020@ubuntu:~/Desktop/project 2$ sudo python pharm_attack.py


IP                       MAC Address
----------------------------------------
10.0.2.3                 08:00:27:73:b3:04
10.0.2.15                08:00:27:44:e1:db
Traceback (most recent call last):
  File "pharm_attack.py", line 275, in <module>
    queue.bind(5, spoof_packet)
  File "netfilterqueue.pyx", line 182, in netfilterqueue.NetfilterQueue.bind (ne
tfilterqueue.c:4388)
OSError: Failed to create queue 5.
cs2020@ubuntu:~/Desktop/project 2$ sudo python pharm_attack.py


IP                       MAC Address
----------------------------------------
10.0.2.3                 08:00:27:73:b3:04
10.0.2.15                08:00:27:44:e1:db
```

ICS [執行中] - Oracle VM VirtualBox

Congrats for finishing DNS spoofing!

Domain Name System (dns), 75 bytes   Packets: 497 · Displayed: 36 (7.2%)   Profile: Default

We can see from the screenshot that we have successfully revisde the DNS packet such that the answer ip has been modified to 140.113.207.246. Consider scenario 2, when attacker (ics2, where the ip is 10.0.2.4) is executing the program, victims(ICS, in this case, the ip is 10.0.2.15) will be redirected to phishing web page if they try to visit www.nctu.edu.tw

三

1. Rely on Virtual Private Networks(VPNs)

2. Encryption
   Protocols such as HTTPS and SSH make it harder for attackers to trick the browser into accepting an illegitimate certificate, thus reduce the chances of a successful ARP poisoning attack.

3. Use a Static ARP :
   Configuring static MAC address in each device or by setting up a static ARP table in the router.

4. Kernel based patches mechanism
   (1)Anticap prevents updating the ARP cache with the existing ARP cache.
   (2)Antidote analyzes the newly received ARP reply with the existing cache. If the previous cache MAC address alive, rejects the new one and adds it to the banned list

5. Tools :
   A third-party tool like XArp for detection.
   ArpWatch : allows notification of MAC/IP changes.
   ArpOn : has a clever caching system apart from the ARP cache that properly allows and denies the packets

6. Set-Up Packet Filtering :
   Packet filters can filter and block malicious packets, as well as those with suspicious IP. They can also tell if a packet claims to come from an internal network when it actually originates externally.

7. Avoid Trust Relationships : such as IP trust relationships