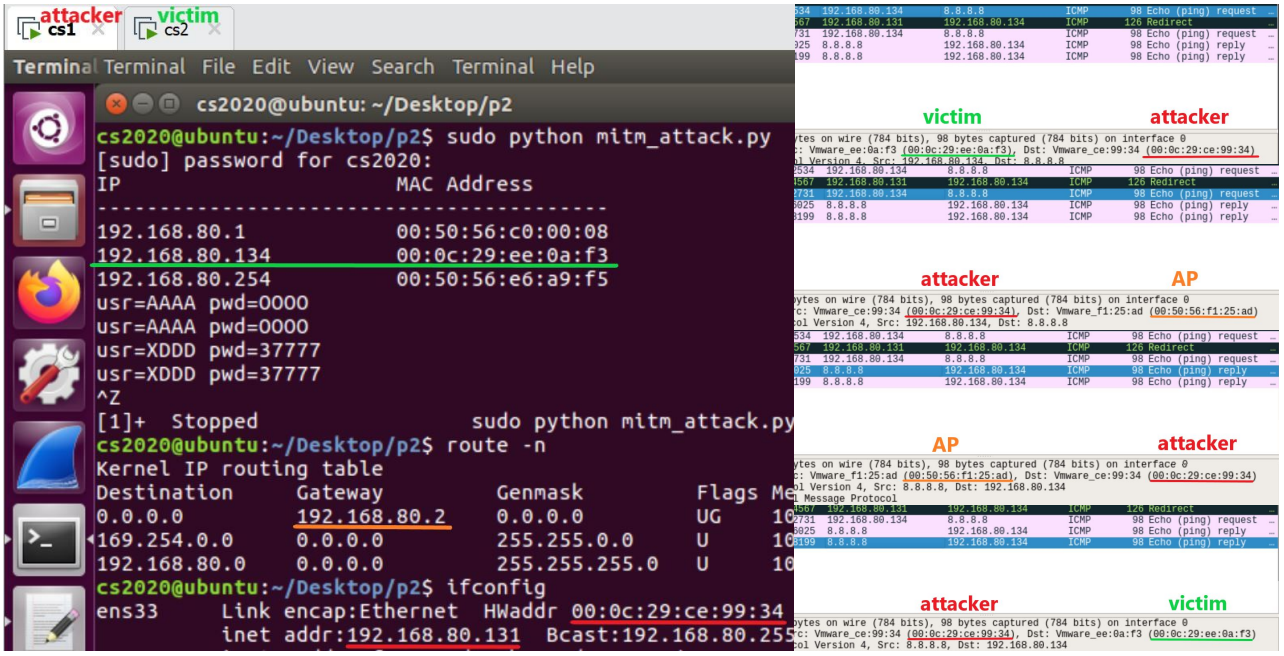
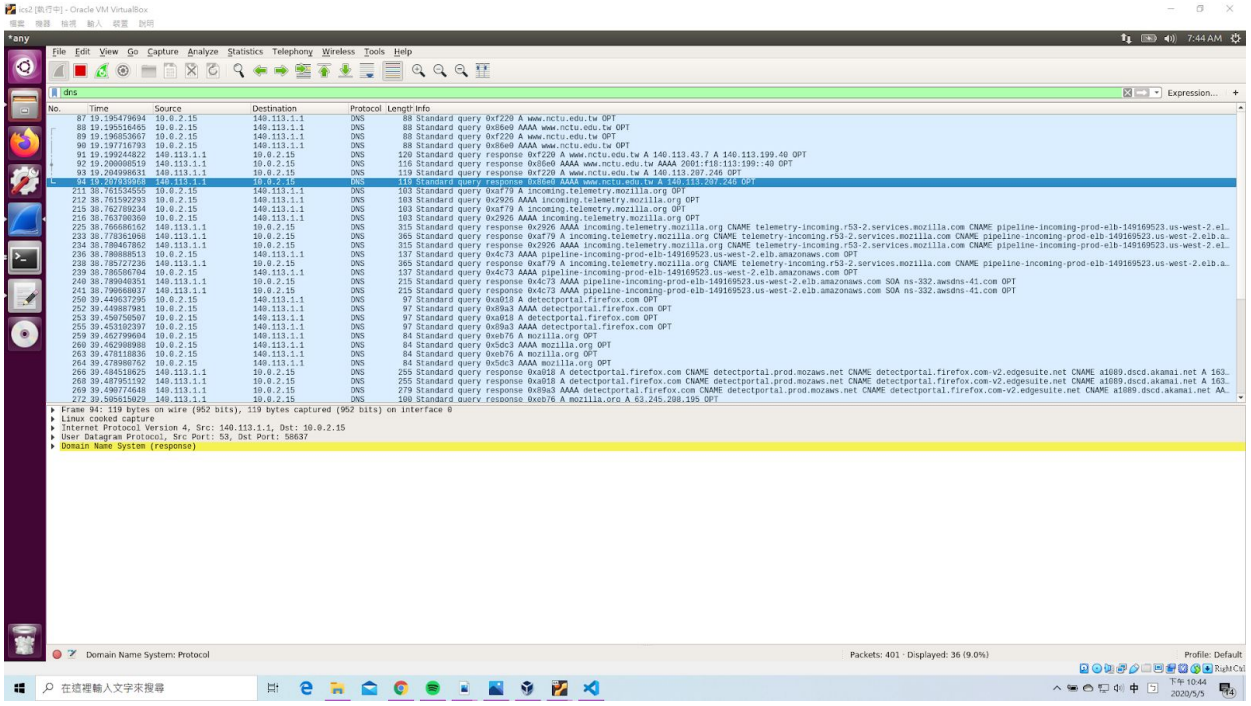
—

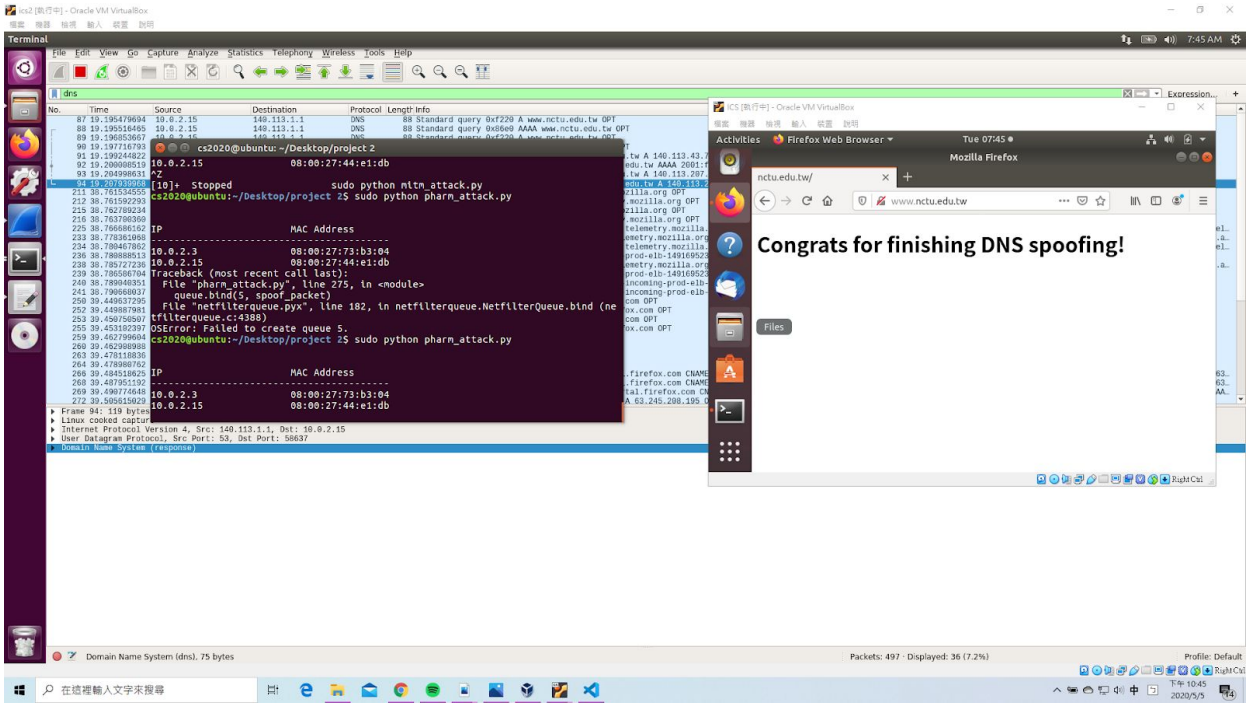


First, get IP/MAC addresses of devices by sending ARP request across our LAN.
Next, send ARP packets with spoofed IP to gateway and victims.
(telling gateway that we are victim and telling victim that we are gateway)
Last, sniff and fetch packets coming from victims, and then print out the retrieved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

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

二





We can see from the screenshot that we have successfully revise the DNS packet where 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 redirect 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