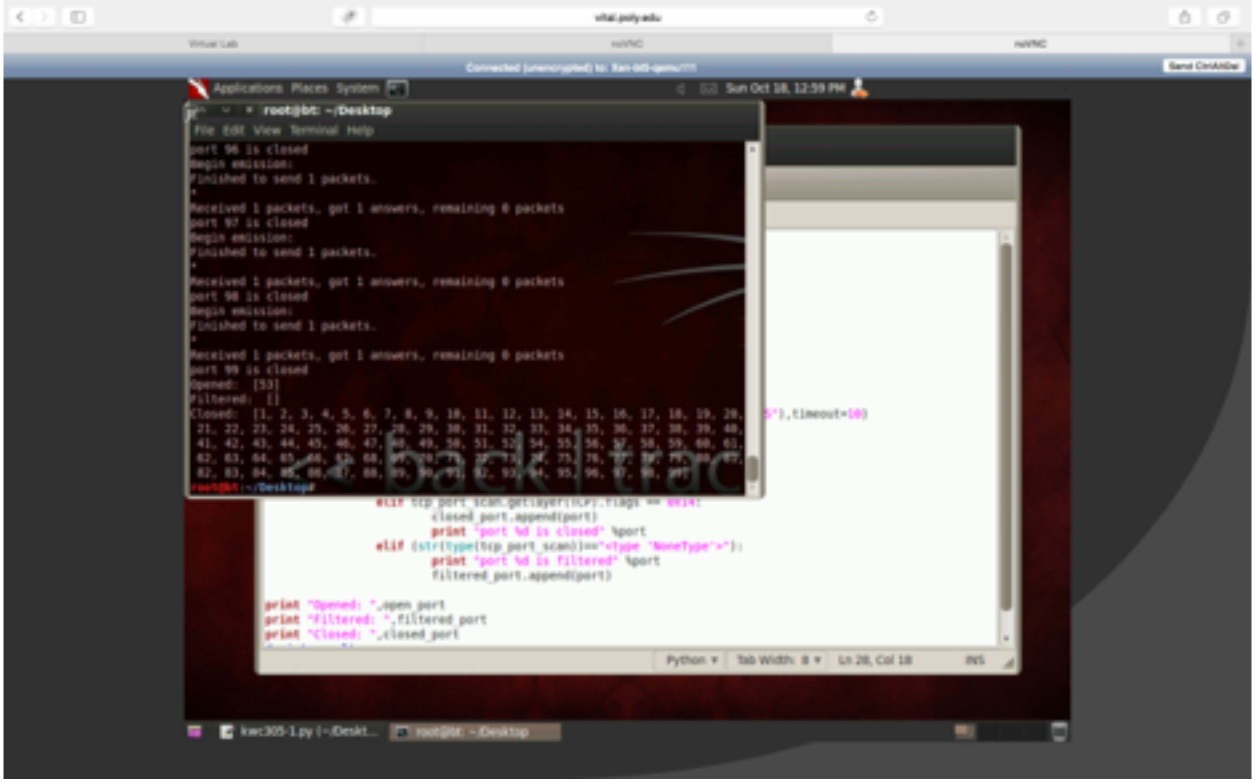
Network Security Lab 3
Kang-Wei Chang
kwc305
N18515255

1.
Your Python TCP scanning program.

See the file kwc305_tcp.py, i use the syn scan, and base on the first packet I received, to see the flags, if the flag is 0x12, it means open, if is 0x14, it means closed, if get type nonetype, it means is filtered in this lab, I received port 53 is open, other is closed.

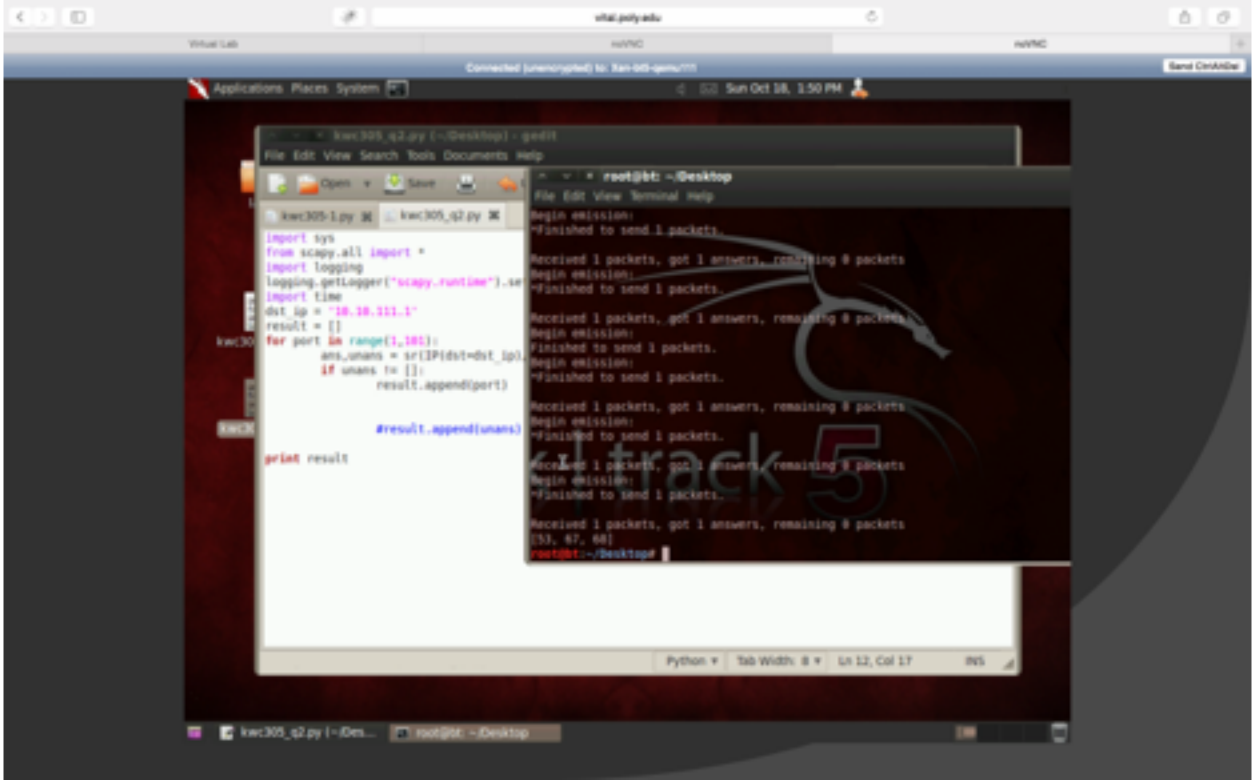


```
port 96 is closed
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
port 97 is closed
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
port 98 is closed
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
port 99 is closed
Opened:  [53]
Filtered:  []
Closed:  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 59, 60, 61,
 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81,
 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99]
root@bt:~/Desktop#
```

```
5"),timeout=10)
```

```
		elif tcp_port_scan.getlayer(TCP).flags == 0x14:
			closed_port.append(port)
			print "port %d is closed" %port
		elif (str(type(tcp_port_scan))=="<type 'NoneType'>"):
			print "port %d is filtered" %port
			filtered_port.append(port)

print "Opened: ",open_port
print "Filtered: ",filtered_port
print "Closed: ",closed_port
```

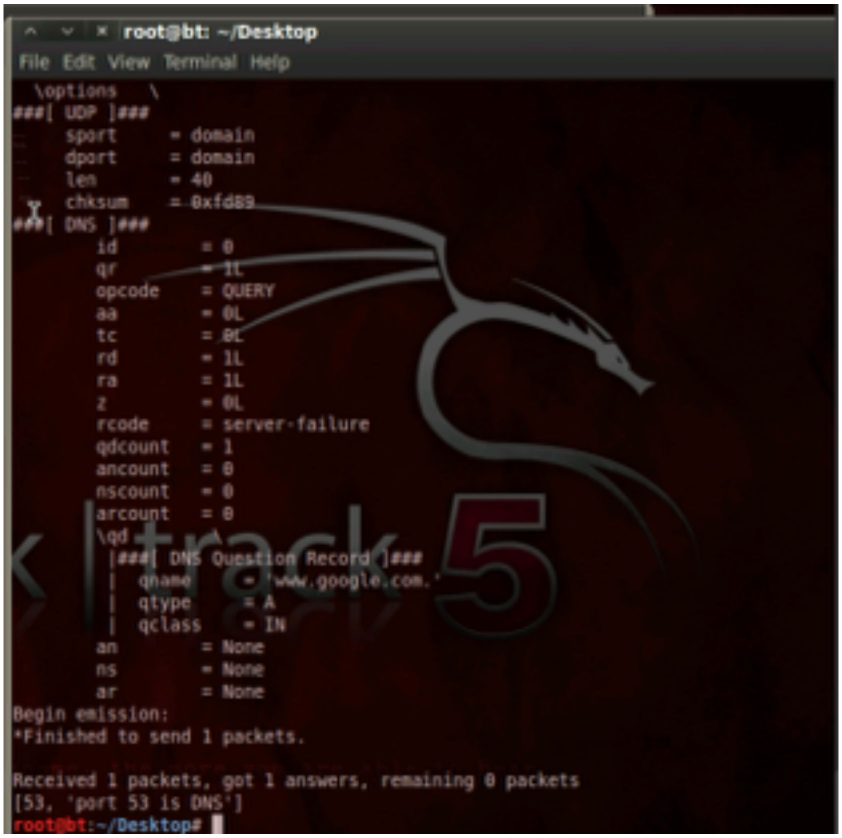
2. UDP scan
See the file kwc305_udp.py. I use the loop to trace the port from 1 to 100. In each sent packet, if there’s any unanswered packet, I will retry to send the packet. If still not reply, than can think is open port. In my code, I got the 53,67,68 are on.



```python
import sys
from scapy.all import *
import logging
logging.getLogger("scapy.runtime").se
import time
dst_ip = "10.10.111.1"
result = []
for port in range(1,101):
        ans,unans = sr(IP(dst=dst_ip),
        if unans != []:
                result.append(port)


                #result.append(unans)


print result
```

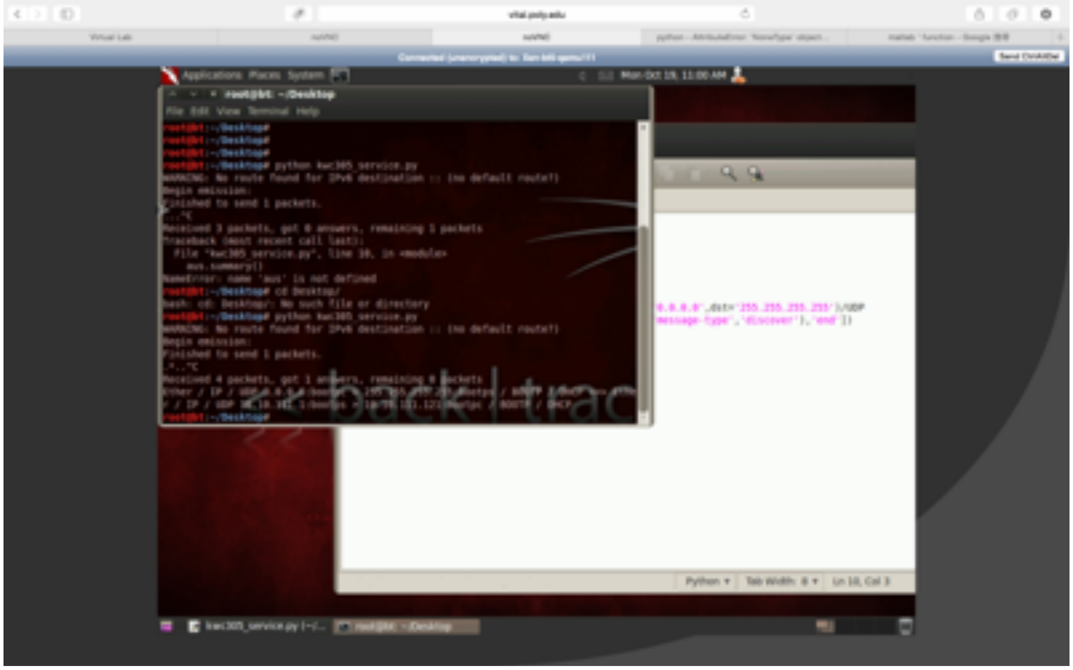
```
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished to send 1 packets.
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
[53, 67, 68]
root@bt:~/Desktop#
```

3. service scan.
See the file kwc305_service.py
Following the udp scan, I already know that the port 53 67 68 are on. Based on the link, I found ports are DNS, Bootstrap Protocol server, Bootstrap Protocol Client.
For the DNS, I also send a DNS packet loop to get the information on the router.



```
  \options   \
###[ UDP ]###
     sport     = domain
     dport     = domain
     len       = 40
     chksum    = 0xfd89
###[ DNS ]###
        id        = 0
        qr        = 1L
        opcode    = QUERY
        aa        = 0L
        tc        = 0L
        rd        = 1L
        ra        = 1L
        z         = 0L
        rcode     = server-failure
        qdcount   = 1
        ancount   = 0
        nscount   = 0
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'www.google.com.'
         |  qtype     = A
         |  qclass    = IN
        an        = None
        ns        = None
        ar        = None
Begin emission:
*Finished to send 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
[53, 'port 53 is DNS']
root@bt:~/Desktop# 
```

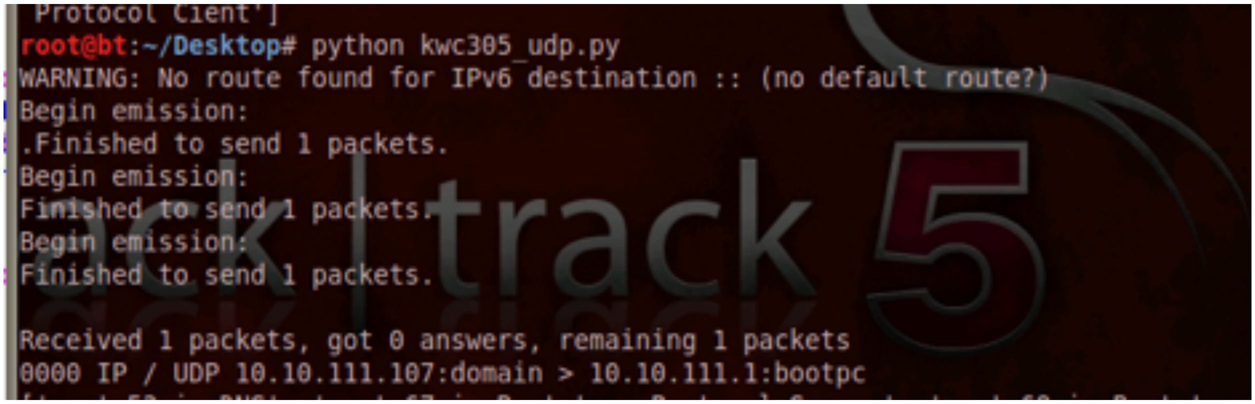
For the port 67: See the file kwc305_dhcp.py
I send a DHCP discover packet and get the following result:



```
root@bt:~/Desktop#
root@bt:~/Desktop#
root@bt:~/Desktop#
root@bt:~/Desktop# python kwc305_service.py
WARNING: No route found for IPv6 destination :: (no default route?)
Begin emission:
Finished to send 1 packets.
...^C
Received 3 packets, got 0 answers, remaining 1 packets
Traceback (most recent call last):
  File "kwc305_service.py", line 10, in <module>
    aus.summary()
NameError: name 'aus' is not defined
root@bt:~/Desktop# cd Desktop/
bash: cd: Desktop/: No such file or directory
root@bt:~/Desktop# python kwc305_service.py
WARNING: No route found for IPv6 destination :: (no default route?)
Begin emission:
Finished to send 1 packets.
.*..^C
Received 4 packets, got 1 answers, remaining 0 packets
Ether / IP / UDP 0.0.0.0:bootpc > 255.255.255.255:bootps / BOOTP / DHCP [illegible]
/ IP / UDP 10.10.101.1:bootps > 10.10.111.121:bootpc / BOOTP / DHCP
root@bt:~/Desktop#
```

```
0.0.0.0',dst='255.255.255.255')/UDP
message-type','discover'),'end')])
```

For the port 68, see the file kwc305_port68.py
I use the and,unans send packet and show the result and found the result:



```
 Protocol Cient']
root@bt:~/Desktop# python kwc305_udp.py
WARNING: No route found for IPv6 destination :: (no default route?)
Begin emission:
.Finished to send 1 packets.
Begin emission:
Finished to send 1 packets.
Begin emission:
Finished to send 1 packets.

Received 1 packets, got 0 answers, remaining 1 packets
0000 IP / UDP 10.10.111.107:domain > 10.10.111.1:bootpc
```