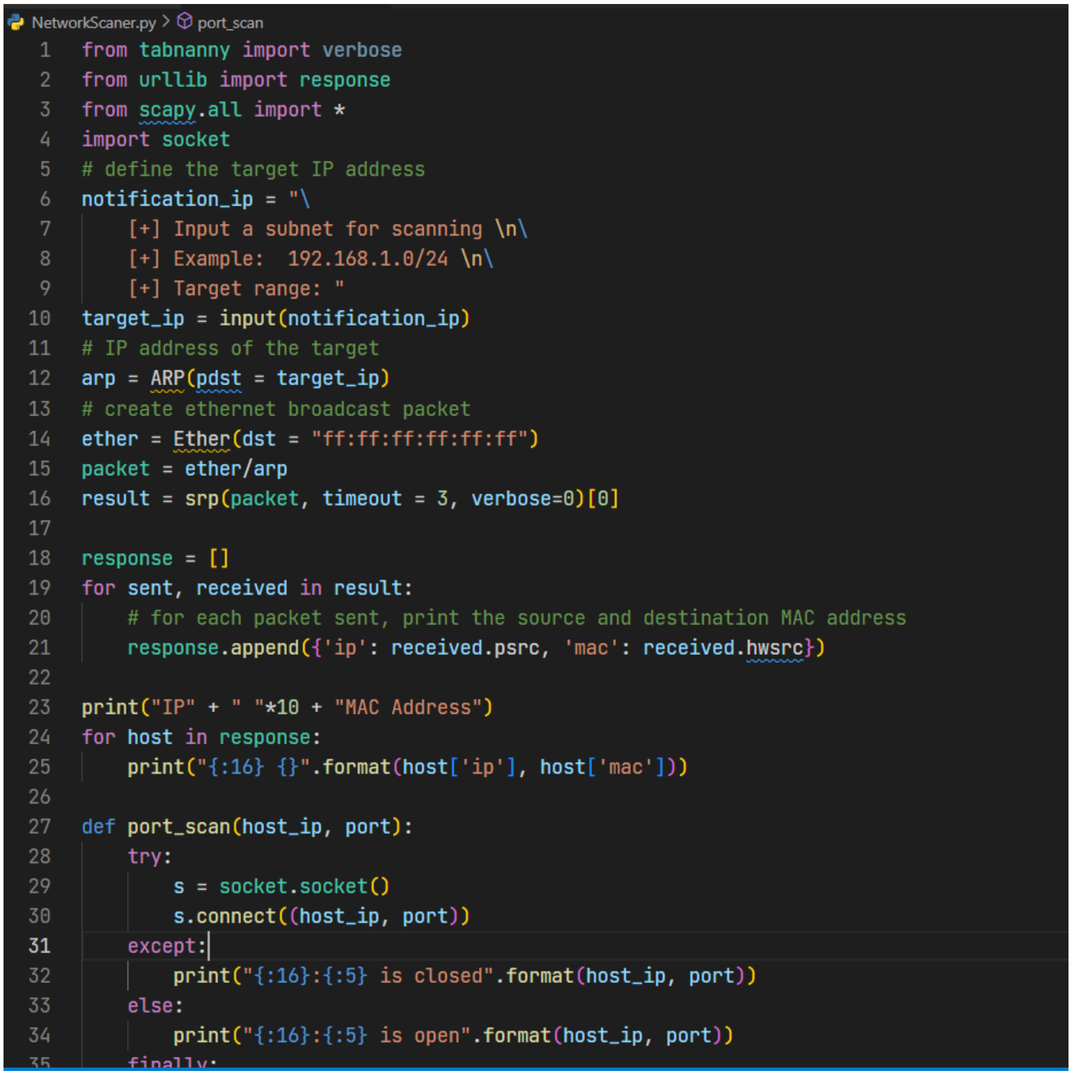
LAB 9

Network Scanner:

Code:

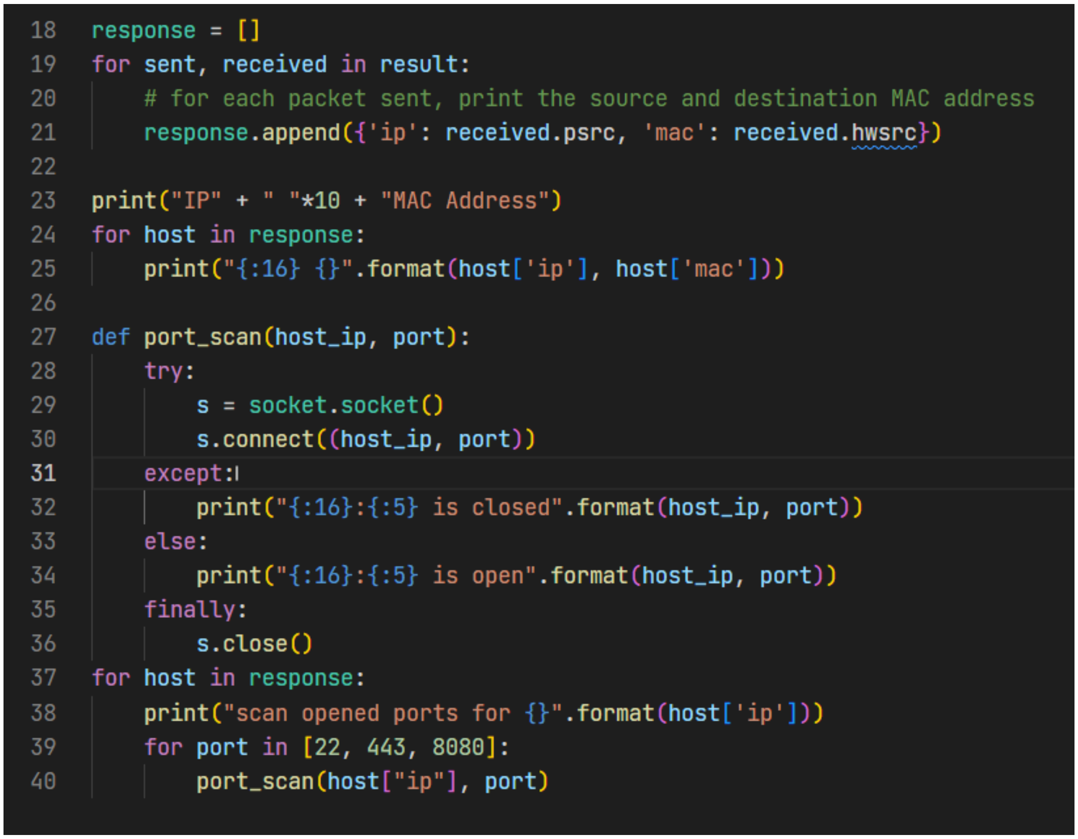


```python
from tabnanny import verbose
from urllib import response
from scapy.all import *
import socket
# define the target IP address
notification_ip = "\
    [+] Input a subnet for scanning \n\
    [+] Example:  192.168.1.0/24 \n\
    [+] Target range: "
target_ip = input(notification_ip)
# IP address of the target
arp = ARP(pdst = target_ip)
# create ethernet broadcast packet
ether = Ether(dst = "ff:ff:ff:ff:ff:ff")
packet = ether/arp
result = srp(packet, timeout = 3, verbose=0)[0]

response = []
for sent, received in result:
    # for each packet sent, print the source and destination MAC address
    response.append({'ip': received.psrc, 'mac': received.hwsrc})

print("IP" + " "*10 + "MAC Address")
for host in response:
    print("{:16} {}".format(host['ip'], host['mac']))

def port_scan(host_ip, port):
    try:
        s = socket.socket()
        s.connect((host_ip, port))
    except:
        print("{:16}:{:5} is closed".format(host_ip, port))
    else:
        print("{:16}:{:5} is open".format(host_ip, port))
    finally:
```

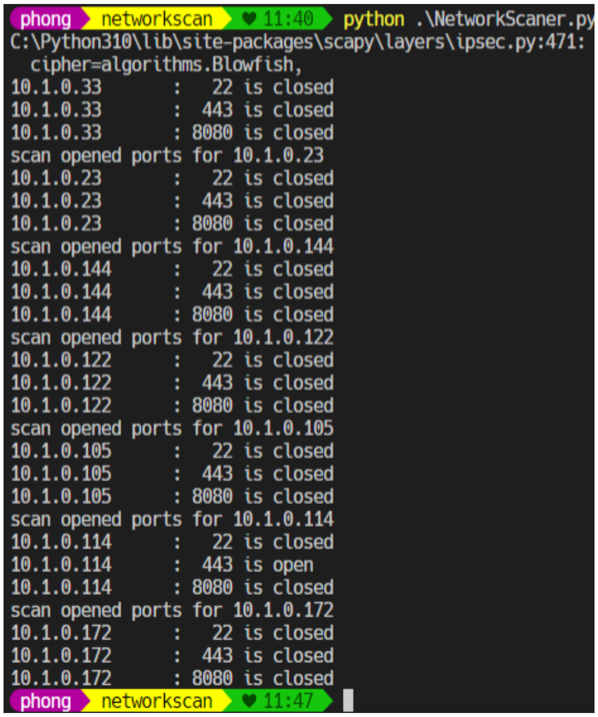


```
response = []
for sent, received in result:
    # for each packet sent, print the source and destination MAC address
    response.append({'ip': received.psrc, 'mac': received.hwsrc})

print("IP" + " "*10 + "MAC Address")
for host in response:
    print("{:16} {}".format(host['ip'], host['mac']))

def port_scan(host_ip, port):
    try:
        s = socket.socket()
        s.connect((host_ip, port))
    except:
        print("{:16}:{:5} is closed".format(host_ip, port))
    else:
        print("{:16}:{:5} is open".format(host_ip, port))
    finally:
        s.close()
for host in response:
    print("scan opened ports for {}".format(host['ip']))
    for port in [22, 443, 8080]:
        port_scan(host["ip"], port)
```

Result:



```
phong  networkscan  ♥ 11:40  python .\NetworkScaner.py
C:\Python310\lib\site-packages\scapy\layers\ipsec.py:471:
  cipher=algorithms.Blowfish,
10.1.0.33       :   22 is closed
10.1.0.33       :  443 is closed
10.1.0.33       : 8080 is closed
scan opened ports for 10.1.0.23
10.1.0.23       :   22 is closed
10.1.0.23       :  443 is closed
10.1.0.23       : 8080 is closed
scan opened ports for 10.1.0.144
10.1.0.144      :   22 is closed
10.1.0.144      :  443 is closed
10.1.0.144      : 8080 is closed
scan opened ports for 10.1.0.122
10.1.0.122      :   22 is closed
10.1.0.122      :  443 is closed
10.1.0.122      : 8080 is closed
scan opened ports for 10.1.0.105
10.1.0.105      :   22 is closed
10.1.0.105      :  443 is closed
10.1.0.105      : 8080 is closed
scan opened ports for 10.1.0.114
10.1.0.114      :   22 is closed
10.1.0.114      :  443 is open
10.1.0.114      : 8080 is closed
scan opened ports for 10.1.0.172
10.1.0.172      :   22 is closed
10.1.0.172      :  443 is closed
10.1.0.172      : 8080 is closed
phong  networkscan  ♥ 11:47
```