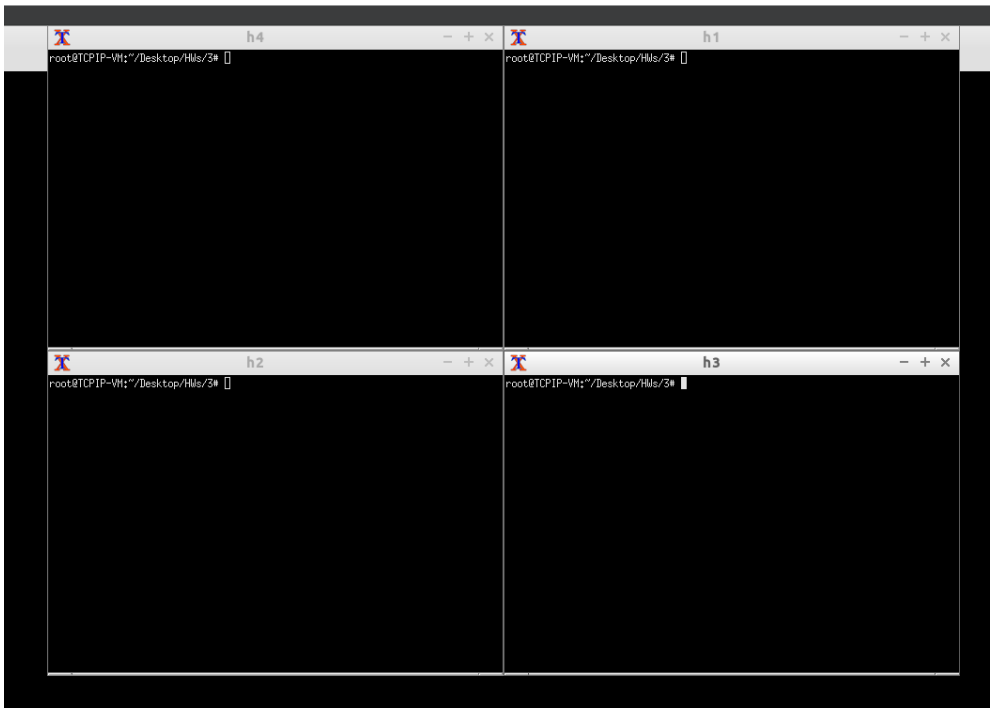
به نام خالق رنگین کمان

ستاره باباجانی – زهرا طباطبائی – گزارش تمرین سوم

الف) ابتدا تغییرات لازم در کد داده شده، انجام شد. سپس با دستور sudo python LabConfig.py کد پایتون اجرا شد:

```
#!/usr/bin/python

"""
This example shows how to create a Mininet object and add nodes to it manually.
"""
"Importing Libraries"
from mininet.net import Mininet
from mininet.node import Controller
from mininet.cli import CLI
from mininet.log import setLogLevel, info
"Function definition: This is called from the main function"
def firstNetwork():
  "Create an empty network and add nodes to it."
  net = Mininet()

  info( '*** Adding controller\n' )
  net.addController( 'c0' )

  info( '*** Adding hosts\n' )
  h1 = net.addHost( 'h1', ip='10.10.14.1/24')
  h2 = net.addHost( 'h2', ip='10.10.24.2/24')
  h3 = net.addHost( 'h3', ip='10.10.34.3/24')
  h4 = net.addHost( 'h4', ip='10.10.14.4/24')

  info( '*** Adding switch\n' )
  s14 = net.addSwitch( 's14' )
  s24 = net.addSwitch( 's24' )
  s34 = net.addSwitch( 's34' )

  info( '*** Creating links\n' )
  net.addLink( h1, s14 )
  net.addLink( h4, s14 )
  net.addLink( h2, s24 )
  net.addLink( h4, s24 )
  net.addLink( h3, s34 )
  net.addLink( h4, s34 )

  h4.cmd('ip addr add 10.10.24.4/24 dev h4-eth1')
  h4.cmd('ip addr add 10.10.34.4/24 dev h4-eth2')
  h4.cmd('echo 1 > /proc/sys/net/ipv4/ip_forward')
  h3.cmd('echo 1 > /proc/sys/net/ipv4/ip_forward')
```

```
    info( '*** Starting network\n')
    net.start()

    info( '*** Adding Gateways\n')
    h1.cmd('ip route add default via 10.10.14.4')
    h2.cmd('ip route add default via 10.10.24.4')
    h3.cmd('ip route add default via 10.10.34.4')

    info( '*** Starting terminals on hosts\n' )
    h1.cmd('xterm -xrm "XTerm.vt100.allowTitleOps: false" -T h1 &')
    h2.cmd('xterm -xrm "XTerm.vt100.allowTitleOps: false" -T h2 &')
    h3.cmd('xterm -xrm "XTerm.vt100.allowTitleOps: false" -T h3 &')
    h4.cmd('xterm -xrm "XTerm.vt100.allowTitleOps: false" -T h4 &')

    info( '*** Running the command line interface\n' )
    CLI( net )

    info( '*** Closing the terminals on the hosts\n' )
    h1.cmd("killall xterm")
    h2.cmd("killall xterm")
    h3.cmd("killall xterm")
    h4.cmd("killall xterm")

    info( '*** Stopping network' )
    net.stop()

"main Function: This is called when the Python file is run"
if __name__ == '__main__':
    setLogLevel( 'info' )
    firstNetwork()
```



ب) برای نشان دادن ping موفق بین Alice, Bank از دستور h1 ping h2 -c5 استفاده میکنیم:

```
mininet> h1 ping h2 -c 5
PING 10.10.24.2 (10.10.24.2) 56(84) bytes of data.
64 bytes from 10.10.24.2: icmp_seq=1 ttl=63 time=3.09 ms
64 bytes from 10.10.24.2: icmp_seq=2 ttl=63 time=0.916 ms
64 bytes from 10.10.24.2: icmp_seq=3 ttl=63 time=0.065 ms
64 bytes from 10.10.24.2: icmp_seq=4 ttl=63 time=0.065 ms
64 bytes from 10.10.24.2: icmp_seq=5 ttl=63 time=0.063 ms

--- 10.10.24.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.063/0.841/3.099/1.176 ms
mininet>
```

مشاهده میشود هر 5 بسته دریافت میشوند و packet loss برابر با 0 است.

ج) با دستور زیر جدول مسیریابی h4 را طوری دستکاری میکنیم تا ترافیک به مقصد بانک را برای سرور مهاجم بفرستد:

```
h4
root@TCPIP-VM:~/Desktop/HWs/3# iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.14.1 -j DNAT --to 10.10.34.3
root@TCPIP-VM:~/Desktop/HWs/3#
```

با استفاده از دستورات زیر، مکانیزم فیلترسازی بر مبنای مسیر معکوس در روتر h4 را فعال میکنیم:

```
root@TCPIP-VM:~/Desktop/HWs/3# echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
root@TCPIP-VM:~/Desktop/HWs/3# echo 0 > /proc/sys/net/ipv4/conf/h4-eth0/rp_filter
root@TCPIP-VM:~/Desktop/HWs/3# echo 0 > /proc/sys/net/ipv4/conf/h4-eth1/rp_filter
root@TCPIP-VM:~/Desktop/HWs/3# echo 0 > /proc/sys/net/ipv4/conf/h4-eth2/rp_filter
root@TCPIP-VM:~/Desktop/HWs/3#
```

د) در ادامه، برای اینکه پاسخ ها ابتدا به h3 برسند، از دستور زیر استفاده میکنیم:

```
root@TCPIP-VM:~/Desktop/HWs/3# iptables -t nat -A POSTROUTING -s 10.10.24.2 -d 10.10.14.1 -j SNAT --to 10.10.34.3
root@TCPIP-VM:~/Desktop/HWs/3#
```

حال باید مبدا بسته ها را به h3 برگردانیم تا h4 متوجه غیرخودی بودن این بسته ها نشود:

h3

```
root@TCPIP-VM:~/Desktop/HWs/3# iptables -t nat -A POSTROUTING -s 10.10.34.3 -d 10.10.14.1 -j SNAT --to 10.10.24.2
root@TCPIP-VM:~/Desktop/HWs/3#
```

سوال 3) خیر زیرا در این صورت امکان ارسال بسته ها به h1 وجود نداشت.

سوال 4) بله، دو راه برای بررسی این موضوع وجود دارد:

1. بررسی rtt: میزان rtt در صورت حمله افزایش می یابد زیرا بسته مسیر طولانی تری را طی میکند.
2. بررسی ttl: مقدار ttl در صورت حمله نسبت به حالت عادی کاهش می یابد زیرا هر بار که بسته از router عبور میکند، ttl آن کاهش می یابد و در حالت حمله، تعداد دفعات عبور بسته از router بیشتر است.