دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

گزارش کار آزمایش ۲

گروه ۴

علی صداقی ۹۷۵۲۱۳۷۸

دانیال بازمانده ۹۷۵۲۱۱۳۵

۱ بخش الف

سوال ۱)

پیاده‌سازی این بخش با تغییرات درون فایل lanConfig.py ایجاد شده است.

```
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('*** Creating links\n')
net.addLink(h1, s14, intfName1="h1-eth0", intfName2="s14-eth1")
net.addLink(h2, s24, intfName1="h2-eth0", intfName2="s24-eth1")
net.addLink(h3, s34, intfName1="h3-eth0", intfName2="s34-eth1")
net.addLink(h4, s14, intfName1="h4-eth0", intfName2="s14-eth2")
net.addLink(h4, s24, intfName1="h4-eth1", intfName2="s24-eth2")
net.addLink(h4, s34, intfName1="h4-eth2", intfName2="s34-eth2")
```

```
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')
```

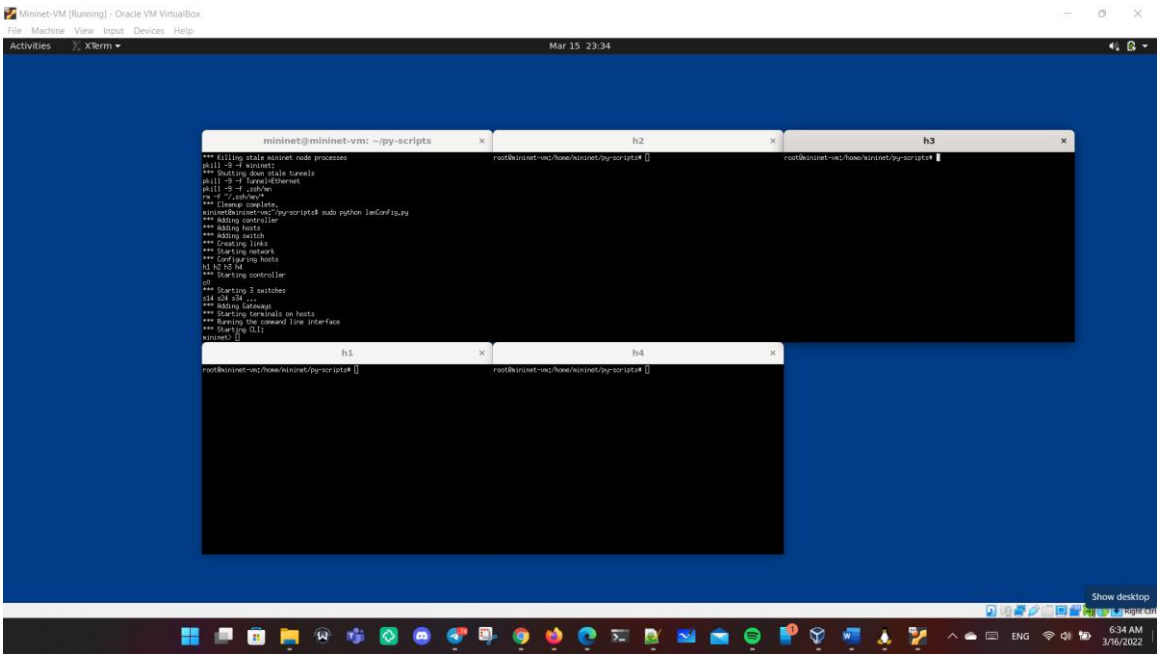
```
info( '*** Adding Gateways\n')
h1.cmd('ip route add default via 10.10.14.4')
h2.cmd('ip route add default via 10.10.24.4')
h3.cmd('ip route add default via 10.10.34.4')
```

از دستور scp برای انتقال این فایل از ماشین لوکال به ماشین مجازی استفاده می‌کنیم.

scp lanConfig.py mininet@192.168.192.3:/home/mininet/py-scripts

شبکه درون فایل را از طریق دستور زیر اجرا می‌کنیم:

sudo python lanConfig.py



۲ سوال ب

مطابق آنچه گفته شد برچسب‌های زیر را برای هر Host در نظر می‌گیریم.

H1 = Bank

H2 = Bob

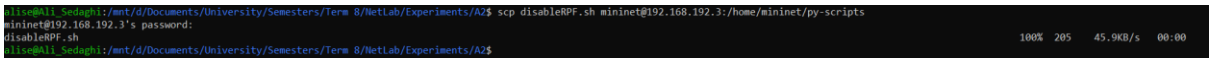
H3 = Attacker

H4 = Router

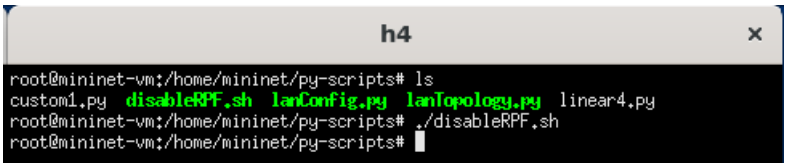
۳ سوال ج

فایل اسکریپت disableRPF.sh که شامل دستورات زیر است را از طریق دستور scp به ماشین مجازی منتقل می‌کنیم.

scp disableRPF.sh mininet@192.168.192.3:/home/mininet/py-scripts

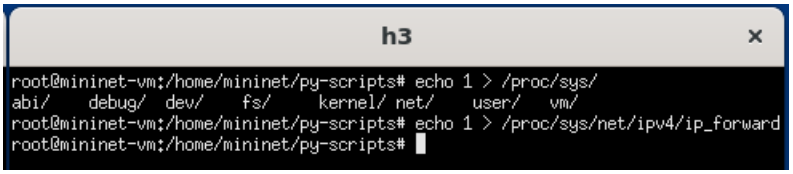


حال این فایل را روی هاست H4 یعنی Router اجرا می‌کنیم.



حال قابلیت IP Forwarding را روی هاست H3 یعنی Attacker فعال می‌کنیم.

echo 1 > /proc/sys/net/ipv4/ip_forward



۴ بخش د

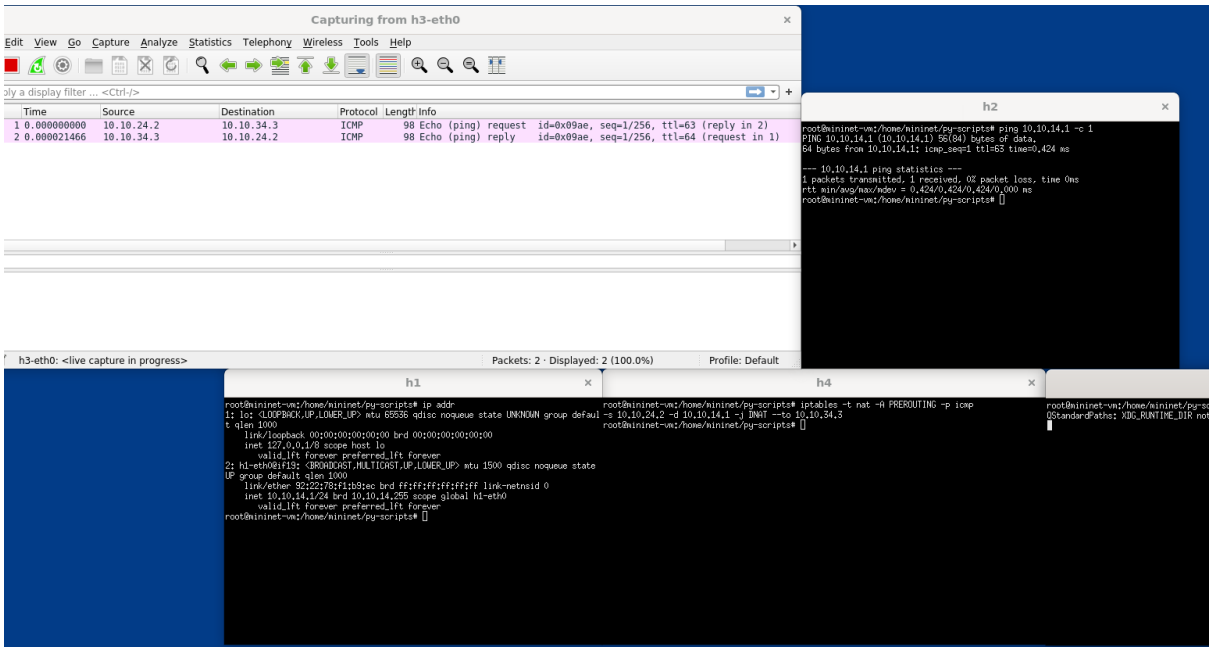
سوال ۲)

ابتدا تنظیم iptables را روی هاست H4 یعنی Router به صورت زیر تغییر می‌دهیم:

```
iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.14.1 -j DNAT --to 10.10.34.3
```

دستور بالا بسته‌های از نوع Ping (ICMP) که از هاست Bob می‌آیند و قرار است به هاست Bank بروند را به هاست Attacker ارسال می‌کند.

اکنون Wireshark را روی هاست H3 یعنی Attacker اجرا می‌کنیم، سپس از هاست H2 یعنی Bob هاست H1 یعنی Bank را پینگ می‌کنیم.



دو بسته Request و Reply از نوع ICMP در H3 یعنی Attacker مشاهده می‌شود.

سوال ۳)

اکنون روی هاست H3 یعنی Attacker باید قوانینی روی iptables تعریف کنیم که بسته ارسالی از Bob به Attacker را با نام Bob به Bank ارسال کنیم.

```
iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.34.3 -j DNAT --to 10.10.14.1
```

پاسخ آن را از Bank بگیریم به Attacker ارسال کنیم سپس از Attacker با نام Bank به Bob ارسال کنیم.

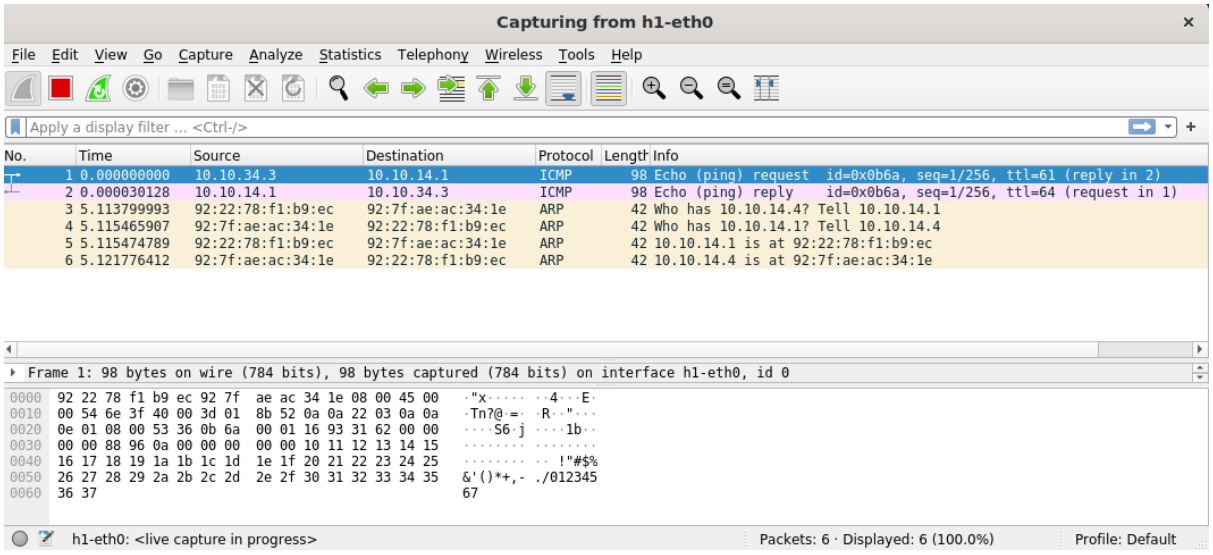
```
iptables -t nat -A POSTROUTING -p icmp -o h3-eth0 -s 10.10.24.2 -j SNAT --to 10.10.34.3
```

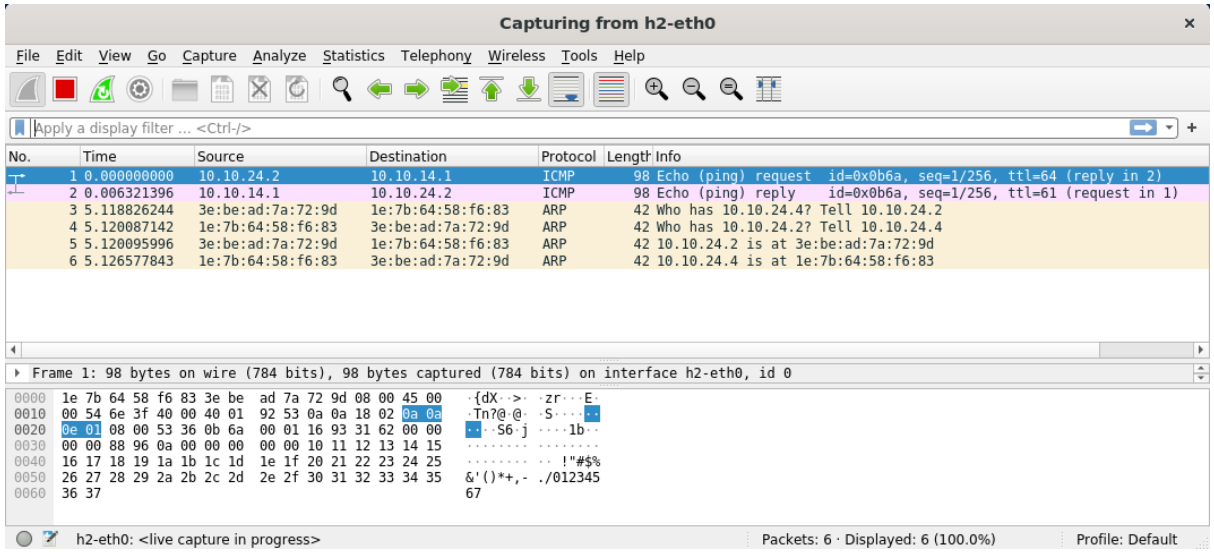
```
h3
root@mininet-vm:/home/mininet/py-scripts# iptables -t nat -A PREROUTING -p icmp
-s 10.10.24.2 -d 10.10.34.3 -j DNAT --to 10.10.14.1
root@mininet-vm:/home/mininet/py-scripts# iptables -t nat -A POSTROUTING -p icmp
 -o h3-eth0 -s 10.10.24.2 -j SNAT --to 10.10.34.3
root@mininet-vm:/home/mininet/py-scripts#
```

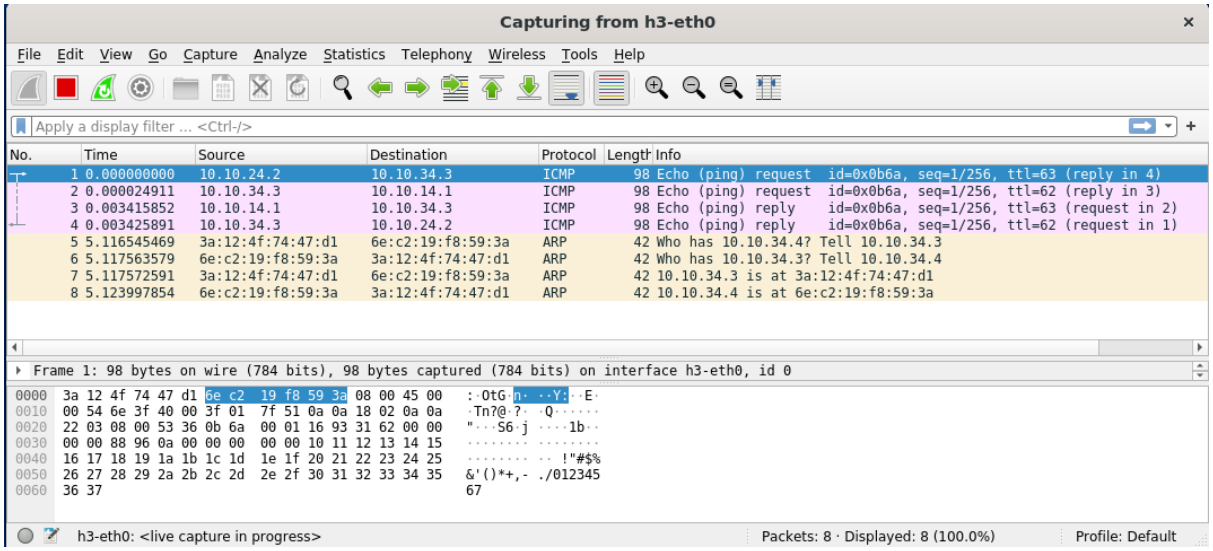
حال Wireshark را روی سه هاست Bob، Bank و Attacker اجرا می‌کنیم و از هاست Bob، Bank را پینگ می‌کنیم.

```
h2
root@mininet-vm:/home/mininet/py-scripts# sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
^Z
[3]+  Stopped                 sudo wireshark
root@mininet-vm:/home/mininet/py-scripts# bg
[3]+ sudo wireshark &
root@mininet-vm:/home/mininet/py-scripts# ping 10.10.14.1 -c 1
PING 10.10.14.1 (10.10.14.1) 56(84) bytes of data.
64 bytes from 10.10.14.1: icmp_seq=1 ttl=61 time=6.35 ms

--- 10.10.14.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.349/6.349/6.349/0.000 ms
root@mininet-vm:/home/mininet/py-scripts#
```







همانطور که مشاهده می‌شود هاست H3 یعنی Attacker توانسته ارتباط Bob (H2) و Bank (H1) را رسد کند بدون اینکه ردی از خود جای بگذارد.

سوال ۴)

خیر. همانطور که در بخش ج عمل کردیم بایستی تغییراتی رو هاست خودمان (Attacker) انجام دهیم تا RPF با Drop کردن بسته‌ها جلوی حمله را نگیرد.

همچنین اگر دو دستور iptables روی هاست Attacker را نمی‌زدیم، بانک و باب متوجه حمله ما می‌شدند زیرا IP متخاصم در پکت‌ها دیده می‌شد.

سوال ۵)

بله. Bob می‌تواند از طریق لاگ‌های درون Router خود متوجه این حمله شود. زیرا IP متخاصم درون Router قابل مشاهده است. همچنین Routerها و مودم‌های جدید دارای قابلیت‌هایی نظیر هستند که جلوی ARP Spoofing یا IP Spoofing را می‌گیرند.