



دانشکده مهندسی کامپیوتر
آزمایشگاه شبکه‌های کامپیوتری

گزارش کار آزمایش ۲

گروه ۴

علی صدیقی 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')
```

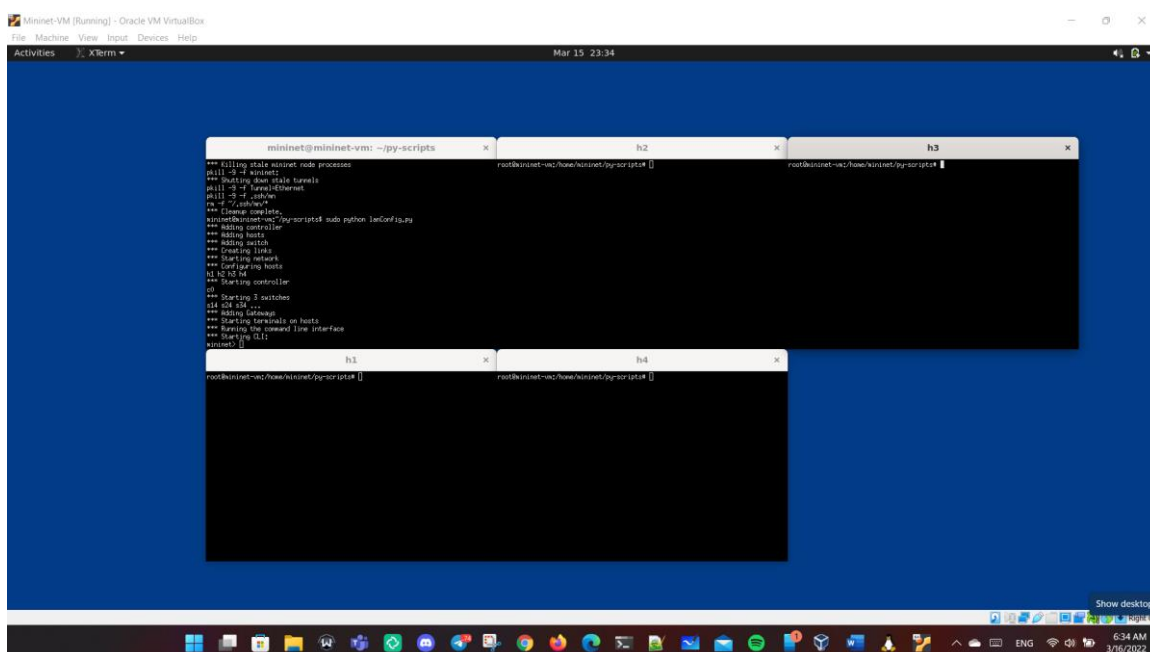
```
info('*** Adding Gateways\n')
h1.cmd('ip route add default via 10.10.14.4')
h2.cmd('ip route add default via 10.10.24.4')
h3.cmd('ip route add default via 10.10.34.4')
```

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 برجسب‌های 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

```
mininet@192.168.192.3:~$ scp disableRPF.sh mininet@192.168.192.3:/home/mininet/py-scripts
mininet@192.168.192.3's password:
disableRPF.sh
mininet@192.168.192.3:~$
```

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

```
h4
root@mininet-vm:/home/mininet/py-scripts# ls
custom1.py  disableRPF.sh  lanConfig.py  lanTopology.py  linear4.py
root@mininet-vm:/home/mininet/py-scripts# ./disableRPF.sh
root@mininet-vm:/home/mininet/py-scripts#
```

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

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

```
h3
root@mininet-vm:/home/mininet/py-scripts# echo 1 > /proc/sys/
abi/  debug/  dev/    fs/     kernel/ net/    user/  vm/
root@mininet-vm:/home/mininet/py-scripts# echo 1 > /proc/sys/net/ipv4/ip_forward
root@mininet-vm:/home/mininet/py-scripts#
```

۴ بخش د

سوال (۲)

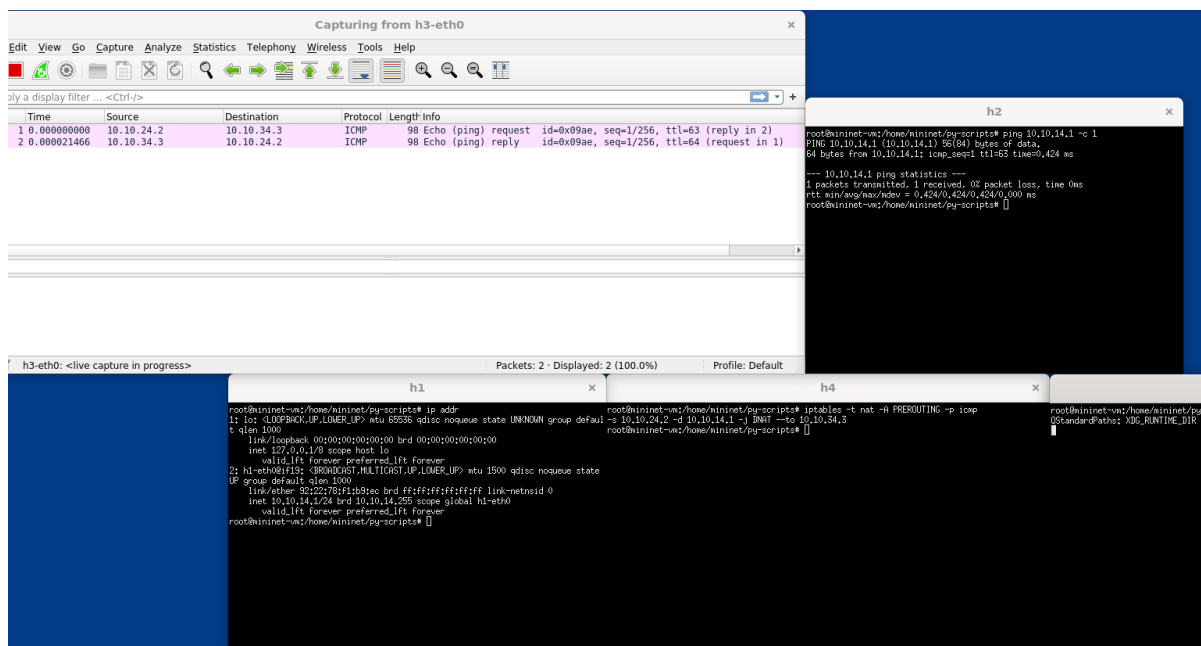
ابتدا تنظیم iptables را روی هاست H4 یعنی Router به صورت زیر تغییر می‌دهیم:

```
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.

```
h4
root@mininet-w1:/home/mininet/py-scripts# 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@mininet-w1:/home/mininet/py-scripts#
```

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#
```

Capturing from h1-eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.34.3	10.10.14.1	ICMP	98	Echo (ping) request id=0x0b6a, seq=1/256, ttl=61 (reply in 2)
2	0.000030128	10.10.14.1	10.10.34.3	ICMP	98	Echo (ping) reply id=0x0b6a, seq=1/256, ttl=64 (request in 1)
3	5.113799993	92:22:78:f1:b9:ec	92:7f:ae:ac:34:1e	ARP	42	Who has 10.10.14.4? Tell 10.10.14.1
4	5.115465907	92:7f:ae:ac:34:1e	92:22:78:f1:b9:ec	ARP	42	Who has 10.10.14.1? Tell 10.10.14.4
5	5.115474789	92:22:78:f1:b9:ec	92:7f:ae:ac:34:1e	ARP	42	10.10.14.1 is at 92:22:78:f1:b9:ec
6	5.121776412	92:7f:ae:ac:34:1e	92:22:78:f1:b9:ec	ARP	42	10.10.14.4 is at 92:7f:ae:ac:34:1e

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface h1-eth0, id 0

0000 92 22 78 f1 b9 ec 92 7f ae ac 34 1e 08 00 45 00 ...x...E..

0010 00 54 6e 3f 40 00 3d 01 8b 52 0a 0a 22 03 0a 0a ...Tn?@-R...

0020 0e 01 08 00 53 36 0b 6a 00 01 16 93 31 62 00 00 ...56.j...1b...

0030 00 00 88 96 0a 00 00 00 00 00 10 11 12 13 14 151b...

0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!#\$%

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345

0060 36 37 67

h1-eth0: <live capture in progress> Packets: 6 · Displayed: 6 (100.0%) Profile: Default

Capturing from h2-eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.24.2	10.10.14.1	ICMP	98	Echo (ping) request id=0x0b6a, seq=1/256, ttl=64 (reply in 2)
2	0.006321396	10.10.14.1	10.10.24.2	ICMP	98	Echo (ping) reply id=0x0b6a, seq=1/256, ttl=61 (request in 1)
3	5.118826244	3e:be:ad:7a:72:9d	1e:7b:64:58:f6:83	ARP	42	Who has 10.10.24.4? Tell 10.10.24.2
4	5.120087142	1e:7b:64:58:f6:83	3e:be:ad:7a:72:9d	ARP	42	Who has 10.10.24.2? Tell 10.10.24.4
5	5.120095996	3e:be:ad:7a:72:9d	1e:7b:64:58:f6:83	ARP	42	10.10.24.2 is at 3e:be:ad:7a:72:9d
6	5.126577843	1e:7b:64:58:f6:83	3e:be:ad:7a:72:9d	ARP	42	10.10.24.4 is at 1e:7b:64:58:f6:83

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface h2-eth0, id 0

0000 1e 7b 64 58 f6 83 3e be ad 7a 72 9d 08 00 45 00 ...{dX->-zr...E..

0010 00 54 6e 3f 40 00 40 01 92 53 0a 0a 18 02 0a 0a ...Tn?@-S...

0020 0e 01 08 00 53 36 0b 6a 00 01 16 93 31 62 00 00 ...56.j...1b...

0030 00 00 88 96 0a 00 00 00 00 00 10 11 12 13 14 151b...

0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25!#\$%

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345

0060 36 37 67

h2-eth0: <live capture in progress> Packets: 6 · Displayed: 6 (100.0%) Profile: Default

Capturing from h3-eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.24.2	10.10.34.3	ICMP	98	Echo (ping) request id=0xb6a, seq=1/256, ttl=63 (reply in 4)
2	0.000024911	10.10.34.3	10.10.14.1	ICMP	98	Echo (ping) request id=0xb6a, seq=1/256, ttl=62 (reply in 3)
3	0.003415852	10.10.14.1	10.10.34.3	ICMP	98	Echo (ping) reply id=0xb6a, seq=1/256, ttl=63 (request in 2)
4	0.003425891	10.10.34.3	10.10.24.2	ICMP	98	Echo (ping) reply id=0xb6a, seq=1/256, ttl=62 (request in 1)
5	5.116545469	3a:12:4f:74:47:d1	6e:c2:19:f8:59:3a	ARP	42	Who has 10.10.34.4? Tell 10.10.34.3
6	5.117563579	6e:c2:19:f8:59:3a	3a:12:4f:74:47:d1	ARP	42	Who has 10.10.34.3? Tell 10.10.34.4
7	5.117572591	3a:12:4f:74:47:d1	6e:c2:19:f8:59:3a	ARP	42	10.10.34.3 is at 3a:12:4f:74:47:d1
8	5.123997854	6e:c2:19:f8:59:3a	3a:12:4f:74:47:d1	ARP	42	10.10.34.4 is at 6e:c2:19:f8:59:3a
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface h3-eth0, id 0						
0000	3a 12 4f 74 47 d1	6e c2 19 f8 59 3a	08 00 45 00	. . OtG n . . . Y: . E .		
0010	00 54 6e 3f 40 00	3f 01 7f 51 0a 0a	18 02 0a 0a	. Tn?@ ? . . Q		
0020	22 03 08 00 53 36	0b 6a 00 01 16 93	31 62 00 00	" . . . S6 . j 1b . .		
0030	00 00 88 96 0a 00	00 00 00 00 00 00	00 00 10 11 12 13		
0040	16 17 18 19 1a 1b	1c 1d 1e 1f 20 21	22 23 24 25 ! "#\$%&		
0050	26 27 28 29 2a 2b	2c 2d 2e 2f 30 31	32 33 34 35	. &' () * + , - . / 01234567		
0060	36 37					

همانطور که مشاهده می‌شود هاست H3 یعنی Attacker توانسته ارتباط (H2) Bob و (H1) Bank 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.