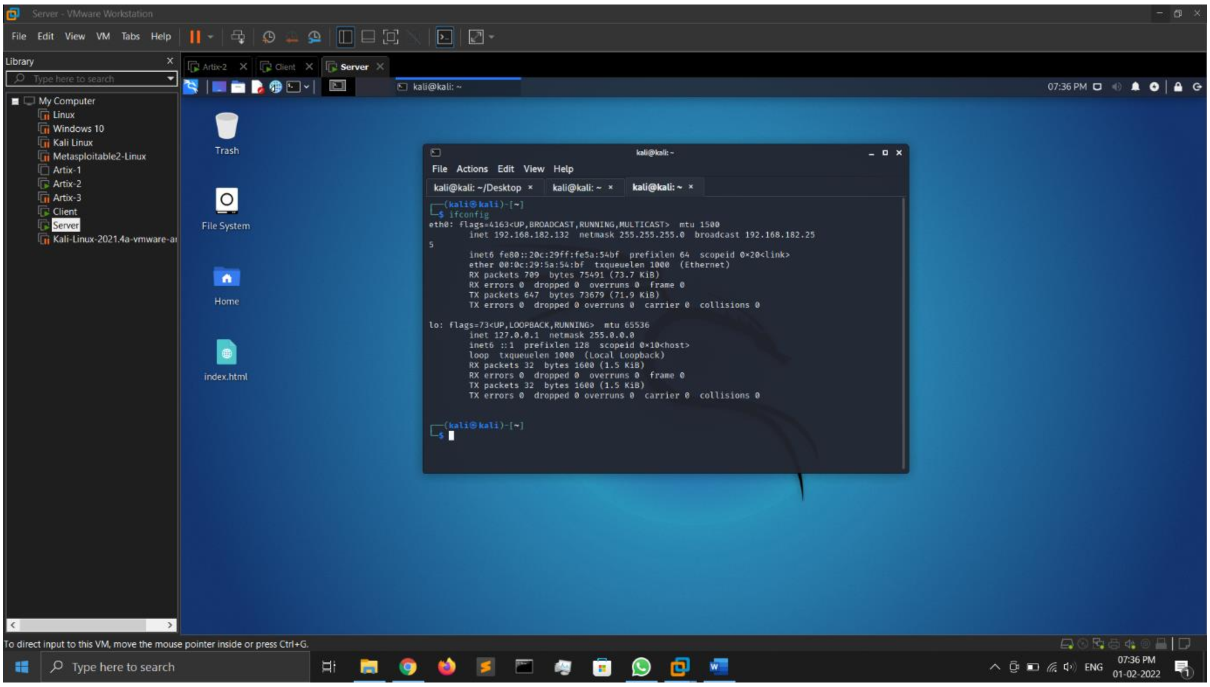
1)

a)

VM3 is connected to interface 192.168.182.0/8, ip assigned – 192.168.182.132

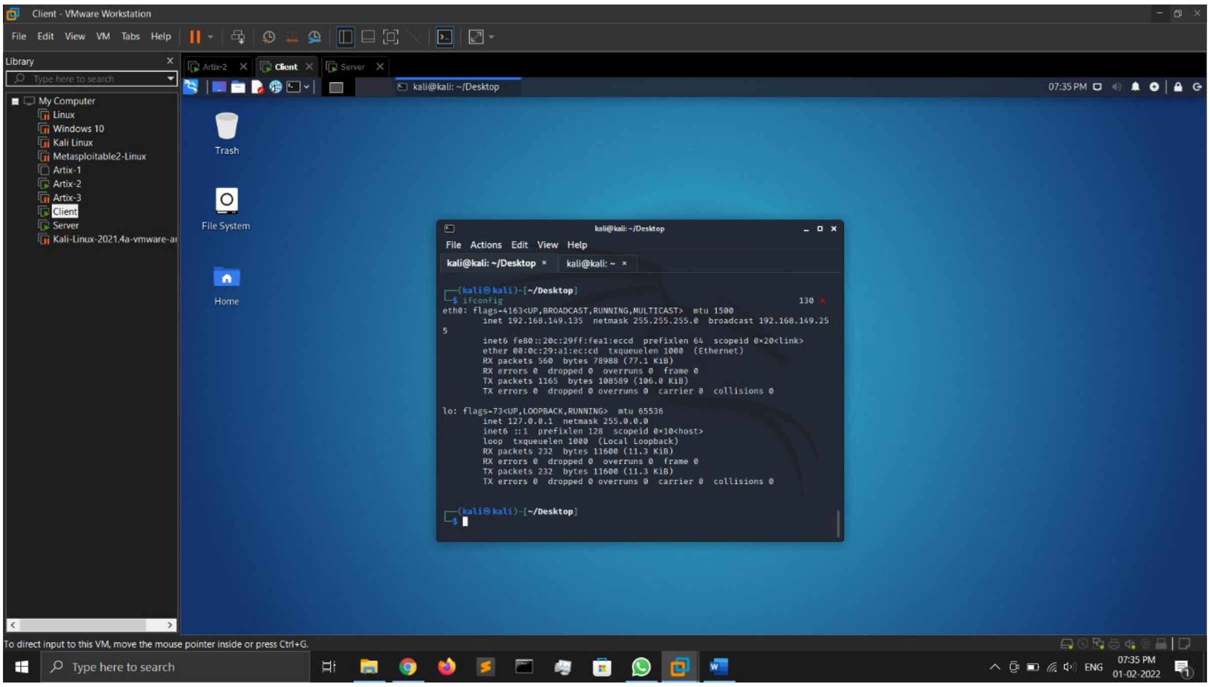


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.182.132  netmask 255.255.255.0  broadcast 192.168.182.25
5
        inet6 fe80::20c:29ff:fe5a:54bf  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:5a:54:bf  txqueuelen 1000  (Ethernet)
        RX packets 709  bytes 75491 (73.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 647  bytes 73679 (71.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1600 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1600 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

VM1 is connected to interface 192.168.149.0/8, ip assigned – 192.168.149.135

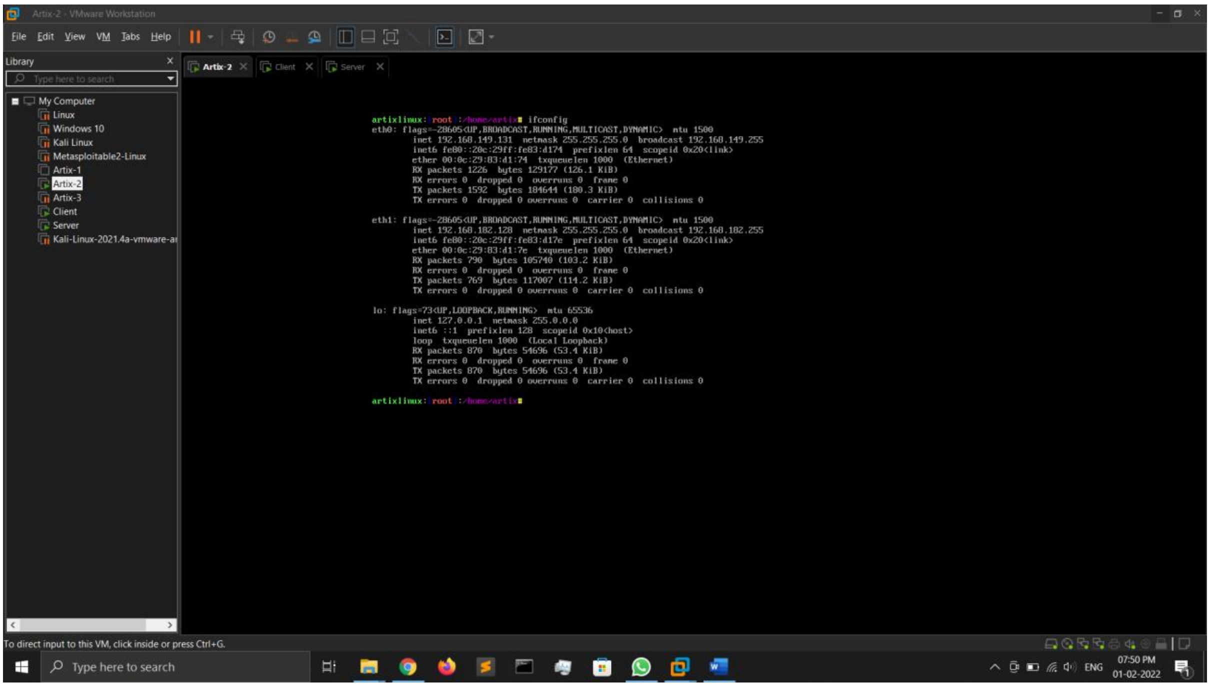


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig                                                       130 ⨯
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.149.135  netmask 255.255.255.0  broadcast 192.168.149.25
5
        inet6 fe80::20c:29ff:fea1:eccd  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:a1:ec:cd  txqueuelen 1000  (Ethernet)
        RX packets 560  bytes 78988 (77.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1165  bytes 108589 (106.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 232  bytes 11600 (11.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 232  bytes 11600 (11.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

VM has 2 subnets 192.168.149.0/8, 192.168.182.0/8 and ips are 192.168.149.131, 192.168.149.128



```
artixlinux:[root]:/home/artix ifconfig
eth0: flags=-28605<UP,BROADCAST,RUNNING,MULTICAST,DYNAMIC>  mtu 1500
        inet 192.168.149.131  netmask 255.255.255.0  broadcast 192.168.149.255
        inet6 fe80::20c:29ff:fe83:d174  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:83:d1:74  txqueuelen 1000  (Ethernet)
        RX packets 1226  bytes 129177 (126.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1592  bytes 184644 (180.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=-28605<UP,BROADCAST,RUNNING,MULTICAST,DYNAMIC>  mtu 1500
        inet 192.168.182.128  netmask 255.255.255.0  broadcast 192.168.182.255
        inet6 fe80::20c:29ff:fe83:d17e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:83:d1:7e  txqueuelen 1000  (Ethernet)
        RX packets 790  bytes 105740 (103.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 769  bytes 117007 (114.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 870  bytes 54696 (53.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 870  bytes 54696 (53.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

artixlinux:[root]:/home/artix
```

b)

On VM1

1. route add -host 192.168.182.132 gw 192.168.149.131

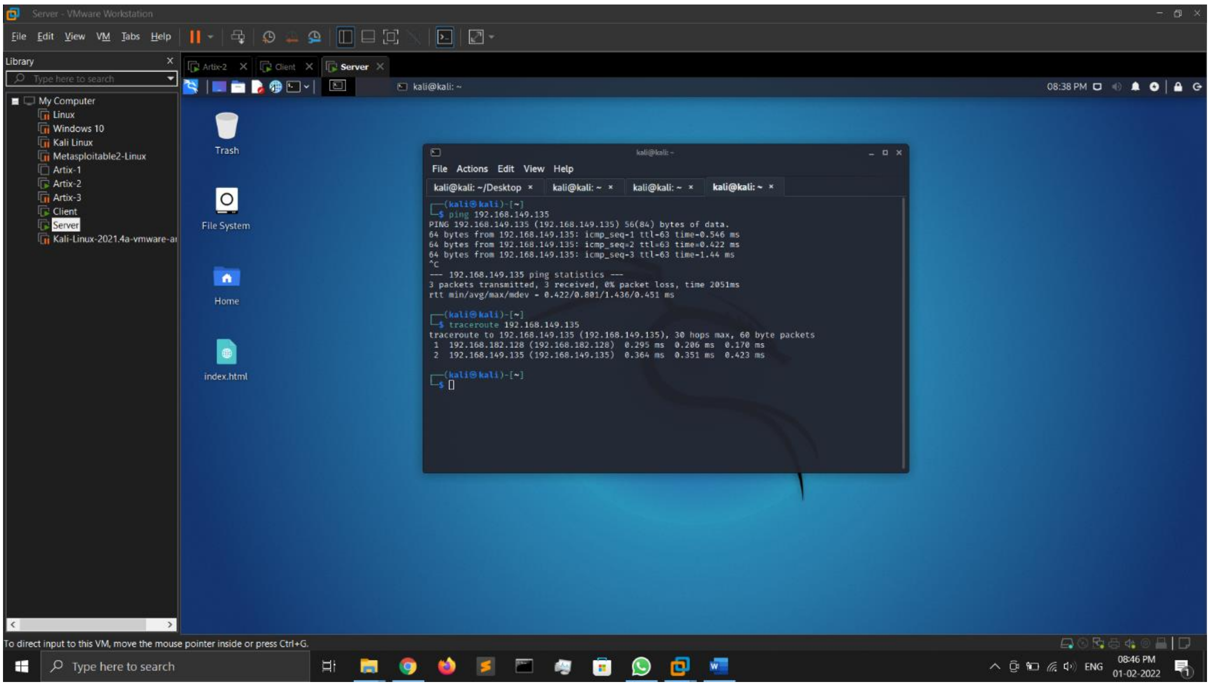
On VM2

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

On VM3

1. route add -host 192.168.149.135 gw 192.168.182.128

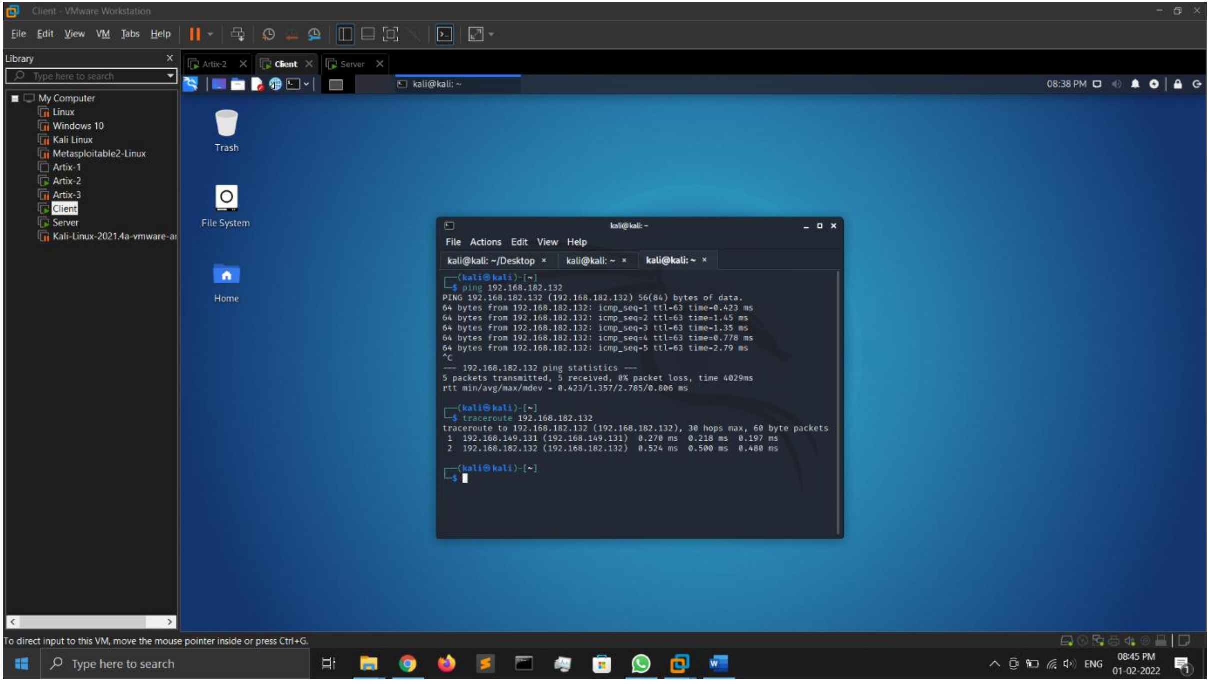
Now we can ping and traceroute VM3 from VM1 and vice-versa



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.149.135
PING 192.168.149.135 (192.168.149.135) 56(84) bytes of data.
64 bytes from 192.168.149.135: icmp_seq=1 ttl=63 time=0.546 ms
64 bytes from 192.168.149.135: icmp_seq=2 ttl=63 time=0.422 ms
64 bytes from 192.168.149.135: icmp_seq=3 ttl=63 time=1.44 ms
^C
--- 192.168.149.135 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.422/0.801/1.436/0.451 ms

┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.149.135
traceroute to 192.168.149.135 (192.168.149.135), 30 hops max, 60 byte packets
 1  192.168.182.128 (192.168.182.128)  0.295 ms  0.206 ms  0.170 ms
 2  192.168.149.135 (192.168.149.135)  0.364 ms  0.351 ms  0.423 ms

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.182.132
PING 192.168.182.132 (192.168.182.132) 56(84) bytes of data.
64 bytes from 192.168.182.132: icmp_seq=1 ttl=63 time=0.423 ms
64 bytes from 192.168.182.132: icmp_seq=2 ttl=63 time=1.45 ms
64 bytes from 192.168.182.132: icmp_seq=3 ttl=63 time=1.35 ms
64 bytes from 192.168.182.132: icmp_seq=4 ttl=63 time=0.778 ms
64 bytes from 192.168.182.132: icmp_seq=5 ttl=63 time=2.79 ms
^C
--- 192.168.182.132 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4029ms
rtt min/avg/max/mdev = 0.423/1.357/2.785/0.806 ms

┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.182.132
traceroute to 192.168.182.132 (192.168.182.132), 30 hops max, 60 byte packets
 1  192.168.149.131 (192.168.149.131)  0.270 ms  0.218 ms  0.197 ms
 2  192.168.182.132 (192.168.182.132)  0.524 ms  0.500 ms  0.480 ms

┌──(kali㉿kali)-[~]
└─$ 
```

c)

I am using python’s simple http server for server.

I have created simple html boilerplate code and am serving it using the command –

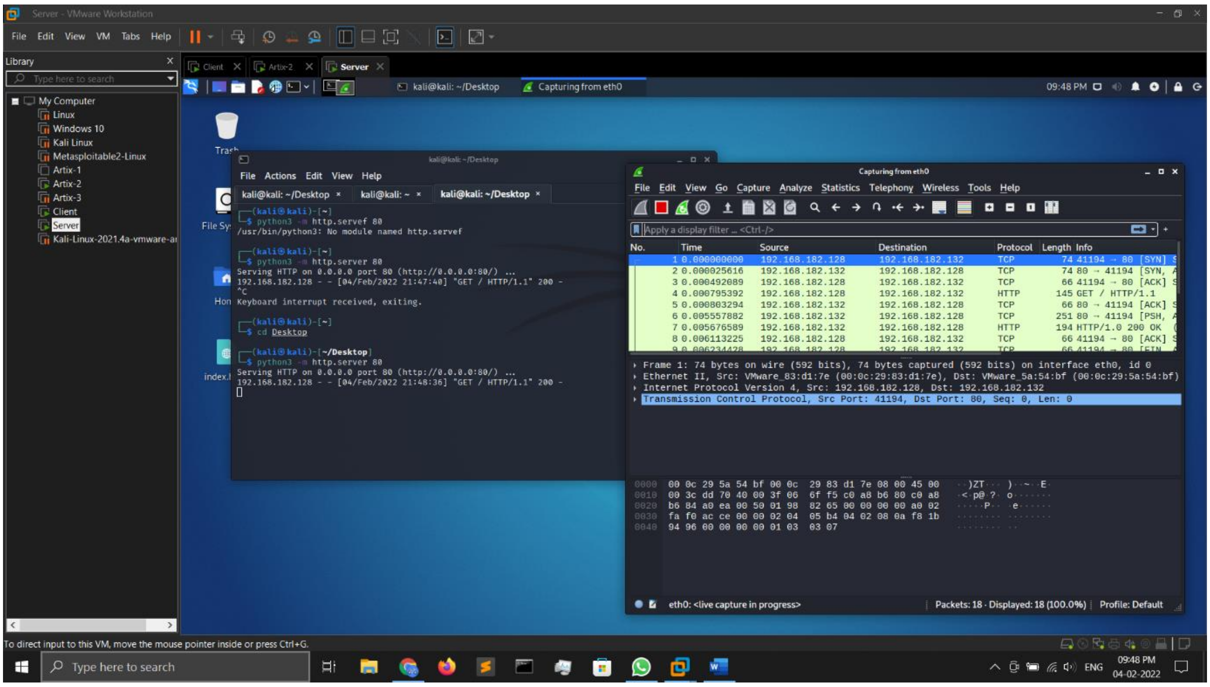
python3 -m http.server 80

d)

Configuring VM2

1) iptables -t nat -A PREROUTING -p tcp -j DNAT --to-destination 192.168.182.132
2) iptables -t nat -A POSTROUTING -p tcp -j SNAT –to-source 192.168.182.128
3) echo 1 > /proc/sys/net/ipv4/ip_forwarding

On VM3



```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.servef 80
/usr/bin/python3: No module named http.servef

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.182.128 - - [04/Feb/2022 21:47:40] "GET / HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.182.128 - - [04/Feb/2022 21:48:36] "GET / HTTP/1.1" 200 -
```

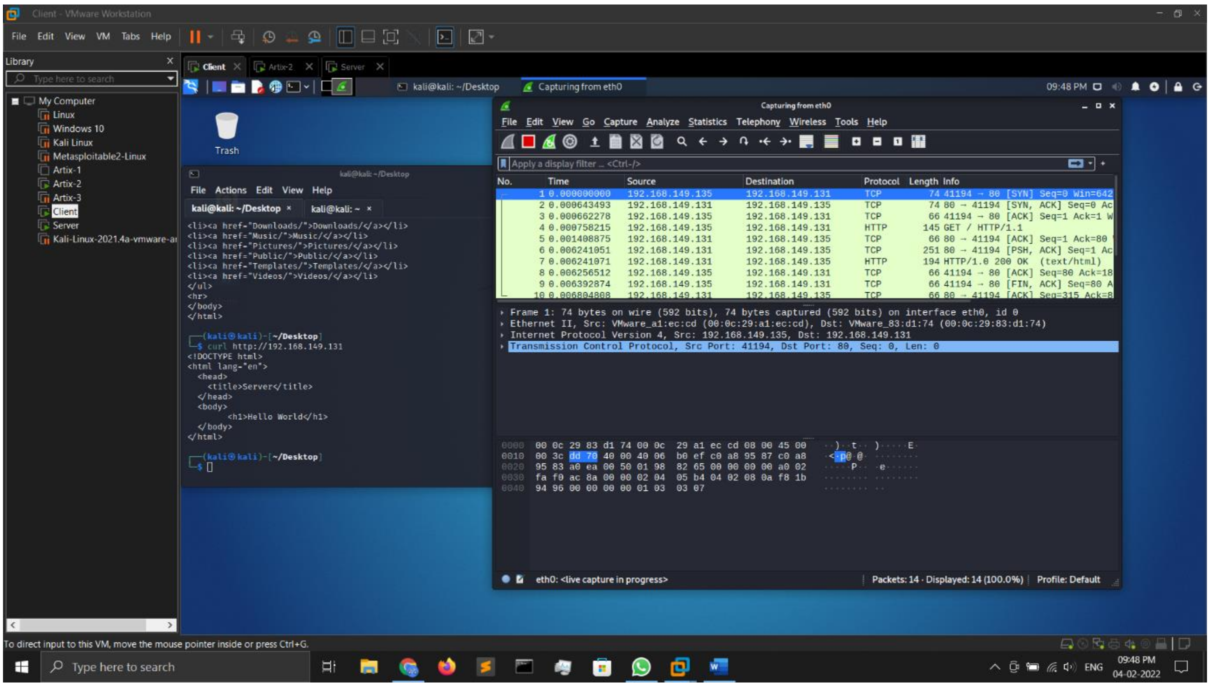
```
No. Time          Source           Destination      Protocol Length Info
  1 0.000000000   192.168.182.128  192.168.182.132  TCP        74 41194 → 80 [SYN] S
  2 0.000025616   192.168.182.132  192.168.182.128  TCP        74 80 → 41194 [SYN, A
  3 0.000492089   192.168.182.128  192.168.182.132  TCP        66 41194 → 80 [ACK] S
  4 0.000795392   192.168.182.128  192.168.182.132  HTTP      145 GET / HTTP/1.1
  5 0.000803294   192.168.182.132  192.168.182.128  TCP        66 80 → 41194 [ACK] S
  6 0.005557882   192.168.182.132  192.168.182.128  TCP       251 80 → 41194 [PSH, A
  7 0.005676589   192.168.182.132  192.168.182.128  HTTP      194 HTTP/1.0 200 OK  (
  8 0.006113225   192.168.182.128  192.168.182.132  TCP        66 41194 → 80 [ACK] S

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_83:d1:7e (00:0c:29:83:d1:7e), Dst: VMware_5a:54:bf (00:0c:29:5a:54:bf)
▸ Internet Protocol Version 4, Src: 192.168.182.128, Dst: 192.168.182.132
▸ Transmission Control Protocol, Src Port: 41194, Dst Port: 80, Seq: 0, Len: 0

0000  00 0c 29 5a 54 bf 00 0c  29 83 d1 7e 08 00 45 00
0010  00 3c dd 70 40 00 3f 06  6f f5 c0 a8 b6 80 c0 a8
0020  b6 84 a0 ea 00 50 01 98  82 65 00 00 00 00 a0 02
0030  fa f0 ac ce 00 00 02 04  05 b4 04 02 08 0a f8 1b
0040  94 96 00 00 00 00 01 03  03 07

eth0: <live capture in progress>    Packets: 18 · Displayed: 18 (100.0%)    Profile: Default
```

On VM1



```
<li><a href="Downloads/">Downloads/</a></li>
<li><a href="Music/">Music/</a></li>
<li><a href="Pictures/">Pictures/</a></li>
<li><a href="Public/">Public/</a></li>
<li><a href="Templates/">Templates/</a></li>
<li><a href="Videos/">Videos/</a></li>
</ul>
<hr>
</body>
</html>

┌──(kali㉿kali)-[~/Desktop]
└─$ curl http://192.168.149.131
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Server</title>
  </head>
  <body>
        <h1>Hello World</h1>
  </body>
</html>

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

```
No. Time          Source           Destination      Protocol Length Info
  1 0.000000000   192.168.149.135  192.168.149.131  TCP        74 41194 → 80 [SYN] Seq=0 Win=642
  2 0.000643493   192.168.149.131  192.168.149.135  TCP        74 80 → 41194 [SYN, ACK] Seq=0 Ac
  3 0.000662278   192.168.149.135  192.168.149.131  TCP        66 41194 → 80 [ACK] Seq=1 Ack=1 W
  4 0.000758215   192.168.149.135  192.168.149.131  HTTP      145 GET / HTTP/1.1
  5 0.001408875   192.168.149.131  192.168.149.135  TCP        66 80 → 41194 [ACK] Seq=1 Ack=80
  6 0.006241051   192.168.149.131  192.168.149.135  TCP       251 80 → 41194 [PSH, ACK] Seq=1 Ac
  7 0.006241071   192.168.149.131  192.168.149.135  HTTP      194 HTTP/1.0 200 OK  (text/html)
  8 0.006256512   192.168.149.135  192.168.149.131  TCP        66 41194 → 80 [ACK] Seq=80 Ack=18
  9 0.006392874   192.168.149.135  192.168.149.131  TCP        66 41194 → 80 [FIN, ACK] Seq=80 A

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_a1:ec:cd (00:0c:29:a1:ec:cd), Dst: VMware_83:d1:74 (00:0c:29:83:d1:74)
▸ Internet Protocol Version 4, Src: 192.168.149.135, Dst: 192.168.149.131
▸ Transmission Control Protocol, Src Port: 41194, Dst Port: 80, Seq: 0, Len: 0

0000  00 0c 29 83 d1 74 00 0c  29 a1 ec cd 08 00 45 00
0010  00 3c dd 70 40 00 40 06  b0 ef c0 a8 95 87 c0 a8
0020  95 83 a0 ea 00 50 01 98  82 65 00 00 00 00 a0 02
0030  fa f0 ac 8a 00 00 02 04  05 b4 04 02 08 0a f8 1b
0040  94 96 00 00 00 00 01 03  03 07

eth0: <live capture in progress>    Packets: 14 · Displayed: 14 (100.0%)    Profile: Default
```

e)

On VM3, on different terminals

1) python3 -m http.server 443
2) python3 -m http.server 80

On VM2

1) iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.182.132

2) iptables -t nat -A POSTROUTING -p tcp --dport 80 -j SNAT –to-source 192.168.182.128
3) iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 192.168.182.132
4) iptables -t nat -A POSTROUTING -p tcp --dport 443 -j SNAT –to-source 192.168.182.128

f)

On VM2

1) iptables -t nat -A PREROUTING -p tcp -s 192.168.149.132 -d 192.168.149.131 --dport 80 -j DNAT --to-destination 192.168.182.132
2) iptables -t nat -A POSTROUTING -p tcp --dport 80 -j SNAT –to-source 192.168.182.128
3) iptables -t nat -A PREROUTING -p tcp -s 192.168.149.132 -d 192.168.149.131 --dport 443 -j DNAT --to-destination 192.168.182.132
4) iptables -t nat -A POSTROUTING -p tcp --dport 443 -j SNAT –to-source 192.168.182.128

Preventing VM2 from accessing webserver at VM3

5) iptables -A OUTPUT -d 192.168.182.132 -j DROP

2)

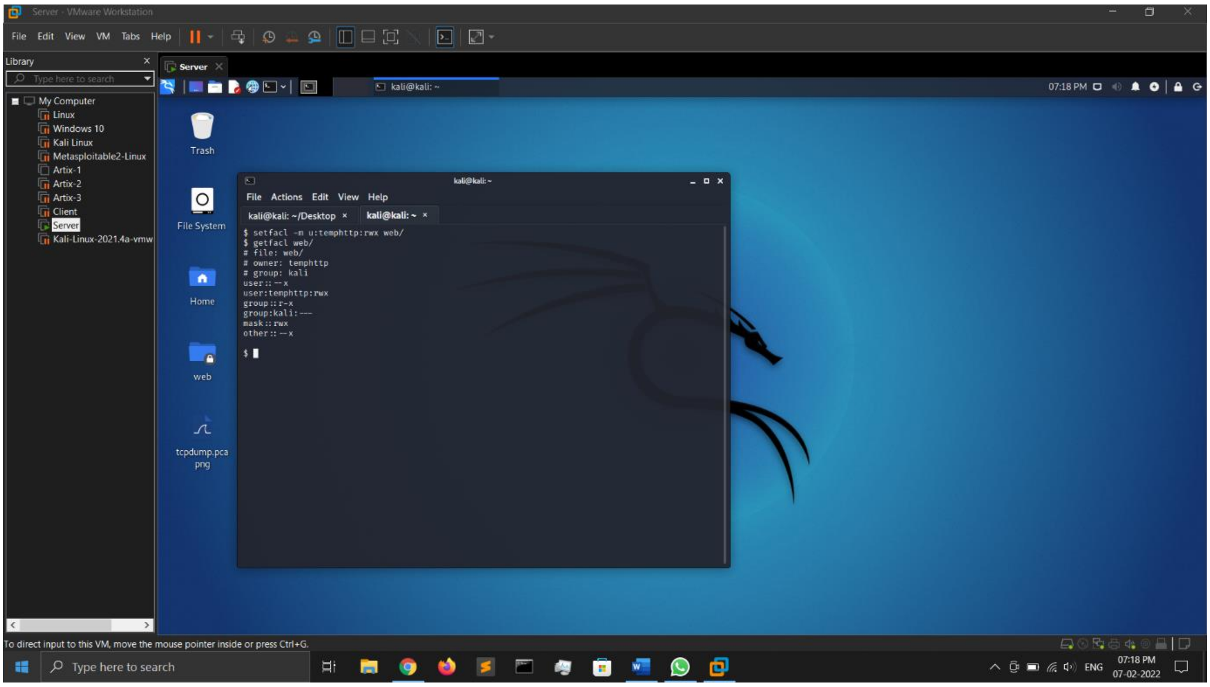
a)

- Created a folder named web and shifted index.html inside it.
- Created user temphttp with command sudo useradd temphttp.
- Changed the owner of temphttp with sudo chown temphttp web
- To revoke read and write access from every process: chmod -R 111 web
- Mode 1 is for execute only.

b) No, “setuid” bit has no effect on directories, it is only used to provide owner level permissions while executing a file. For providing write access to directories, “setgid” bit is used instead.

c) For specific access

- setfacl -m u:temphttp:rwx web/
- As we can see in the screenshot on next page, there has appeared a separated user permissions for temphttp having rwx access



```
$ setfacl -m u:temphttp:rwx web/
$ getfacl web/
# file: web/
# owner: temphttp
# group: kali
user::--x
user:temphttp:rwx
group::r-x
group:kali:---
mask::rwx
other::--x

$ ▌
```