

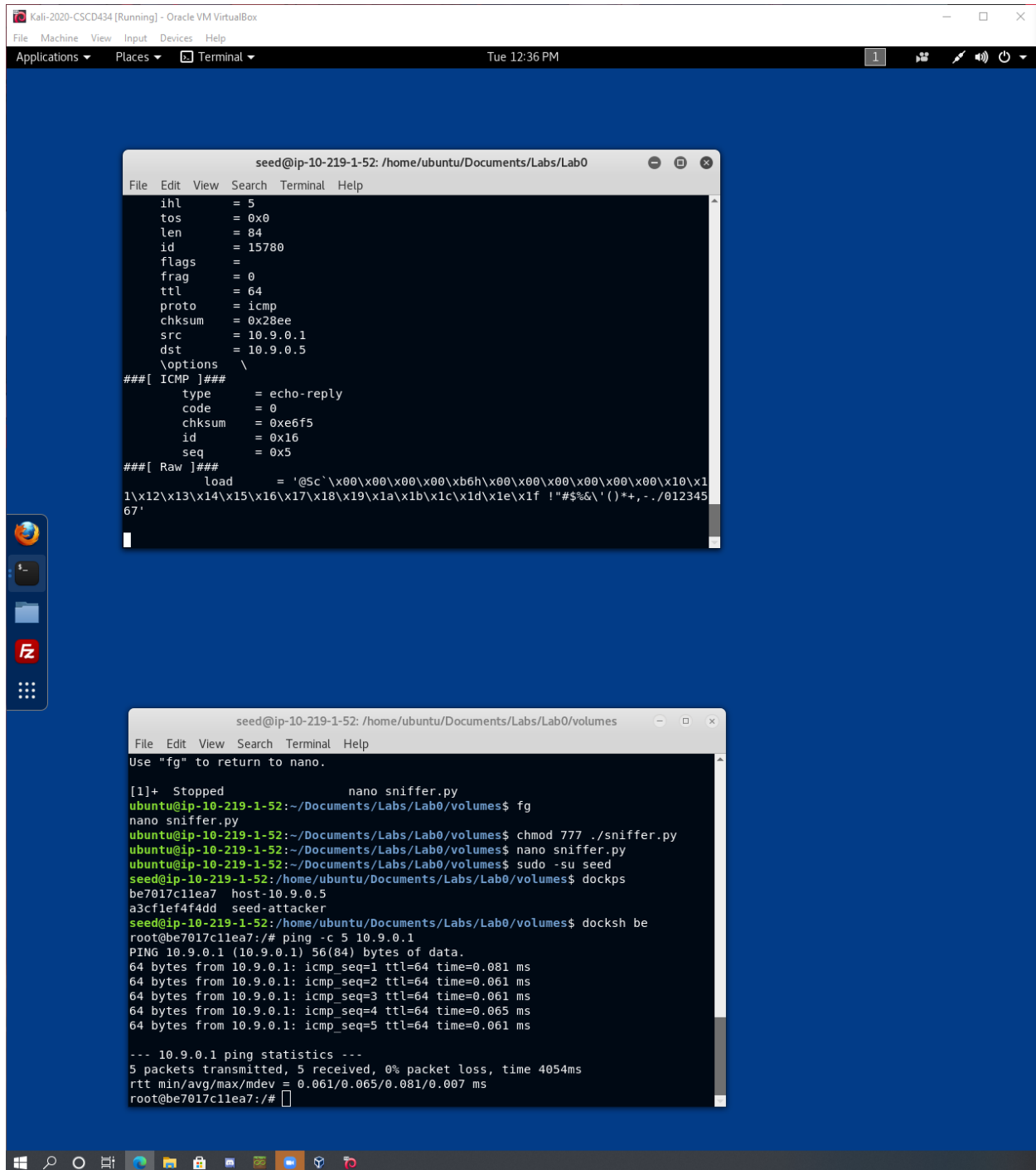
## Lab 0 – AWS Setup and Sniffing

Ian Kaiserman

Screenshot of dockps command

```
seed@ip-10-219-1-52:/home/ubuntu/Documents/Labs/Lab0$ dockps  
be7017c11ea7  host-10.9.0.5  
a3cf1ef4f4dd  seed-attacker
```

## Screenshot of sniffer.py output (window 1) and ping command output (window 2)



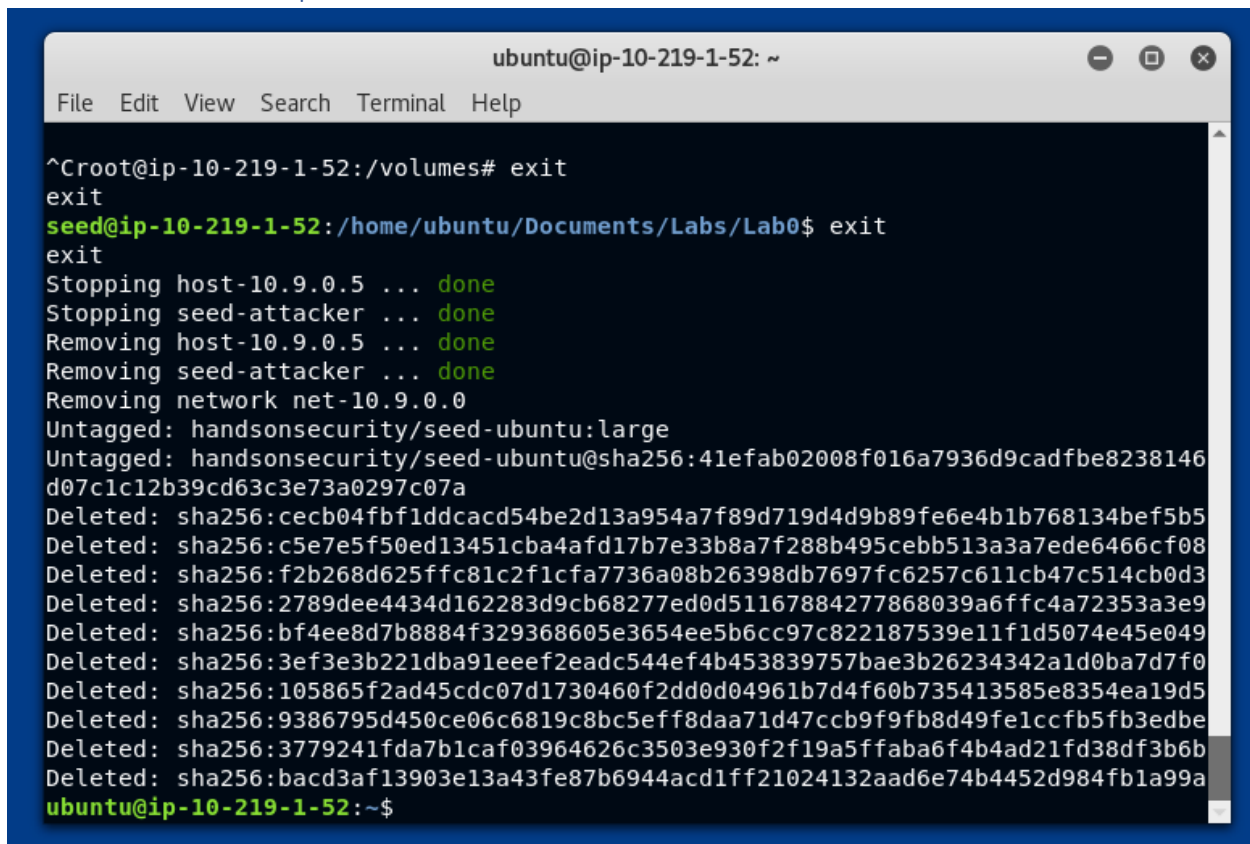
```
seed@ip-10-219-1-52: /home/ubuntu/Documents/Labs/Lab0
File Edit View Search Terminal Help
ihl      = 5
tos      = 0x0
len      = 84
id       = 15780
flags    =
frag     = 0
ttl      = 64
proto    = icmp
checksum = 0x28ee
src      = 10.9.0.1
dst      = 10.9.0.5
\options
\
###[ ICMP ]###
type     = echo-reply
code     = 0
checksum = 0xe6f5
id       = 0x16
seq      = 0x5
###[ Raw ]###
load     = '@Sc'\x00\x00\x00\x00\xb6h\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&'()*+,-./01234567'
```

```
seed@ip-10-219-1-52: /home/ubuntu/Documents/Labs/Lab0/volumes
File Edit View Search Terminal Help
Use "fg" to return to nano.

[1]+  Stopped                  nano sniffer.py
ubuntu@ip-10-219-1-52:~/Documents/Labs/Lab0/volumes$ fg
nano sniffer.py
ubuntu@ip-10-219-1-52:~/Documents/Labs/Lab0/volumes$ chmod 777 ./sniffer.py
ubuntu@ip-10-219-1-52:~/Documents/Labs/Lab0/volumes$ nano sniffer.py
ubuntu@ip-10-219-1-52:~/Documents/Labs/Lab0/volumes$ sudo -su seed
seed@ip-10-219-1-52:/home/ubuntu/Documents/Labs/Lab0/volumes$ dockps
be7017c1lea7 host-10.9.0.5
a3cf1ef4f4dd seed-attacker
seed@ip-10-219-1-52:/home/ubuntu/Documents/Labs/Lab0/volumes$ docksh be
root@be7017c1lea7:/# ping -c 5 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.081 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.061 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.065 ms
64 bytes from 10.9.0.1: icmp_seq=5 ttl=64 time=0.061 ms

--- 10.9.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.061/0.065/0.081/0.007 ms
root@be7017c1lea7:/#
```

## Screenshot of cleanup



```
ubuntu@ip-10-219-1-52: ~  
File Edit View Search Terminal Help  
  
^Croot@ip-10-219-1-52:/volumes# exit  
exit  
seed@ip-10-219-1-52:/home/ubuntu/Documents/Labs/Lab0$ exit  
exit  
Stopping host-10.9.0.5 ... done  
Stopping seed-attacker ... done  
Removing host-10.9.0.5 ... done  
Removing seed-attacker ... done  
Removing network net-10.9.0.0  
Untagged: handsonsecurity/seed-ubuntu:large  
Untagged: handsonsecurity/seed-ubuntu@sha256:41efab02008f016a7936d9cadfbe8238146  
d07c1c12b39cd63c3e73a0297c07a  
Deleted: sha256:cecb04fbf1ddcacd54be2d13a954a7f89d719d4d9b89fe6e4b1b768134bef5b5  
Deleted: sha256:c5e7e5f50ed13451cba4afd17b7e33b8a7f288b495cebb513a3a7ede6466cf08  
Deleted: sha256:f2b268d625ffc81c2f1cfa7736a08b26398db7697fc6257c611cb47c514cb0d3  
Deleted: sha256:2789dee4434d162283d9cb68277ed0d51167884277868039a6ffc4a72353a3e9  
Deleted: sha256:bf4ee8d7b8884f329368605e3654ee5b6cc97c822187539e11fd5074e45e049  
Deleted: sha256:3ef3e3b221dba91eeef2eadc544ef4b453839757bae3b26234342a1d0ba7d7f0  
Deleted: sha256:105865f2ad45cdc07d1730460f2dd0d04961b7d4f60b735413585e8354ea19d5  
Deleted: sha256:9386795d450ce06c6819c8bc5eff8daa71d47ccb9f9fb8d49fe1ccfb5fb3edbe  
Deleted: sha256:3779241fda7b1caf03964626c3503e930f2f19a5ffaba6f4b4ad21fd38df3b6b  
Deleted: sha256:bacd3af13903e13a43fe87b6944acd1ff21024132aad6e74b4452d984fbl99a  
ubuntu@ip-10-219-1-52:~$
```