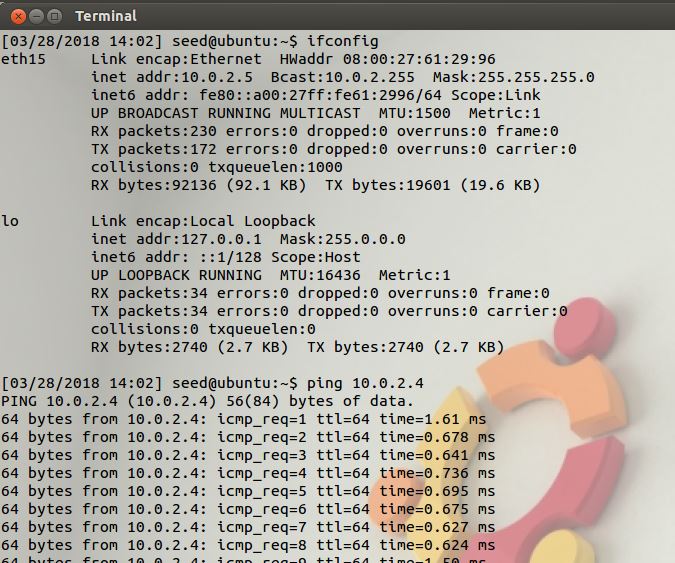
Matt Ritchie

YCP Cyber Security

4-9-18 (PLEASE UPDATE NOT FINISHED)

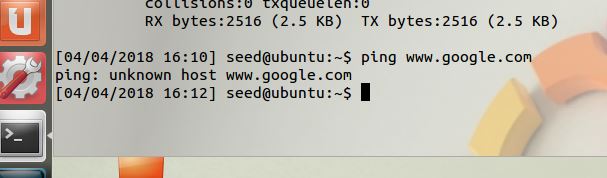
Task 1.

After setting up 3 Ubuntu VMs according to the instructions, which I named Attacker, Victim, and Observer, I tested the connection between them by having Attacker ping Victim.



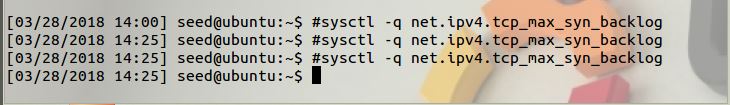
The ping times seemed oddly short, but since they are all VMs living on the same hardware, I figured there was just a lot less the pings had to travel through.

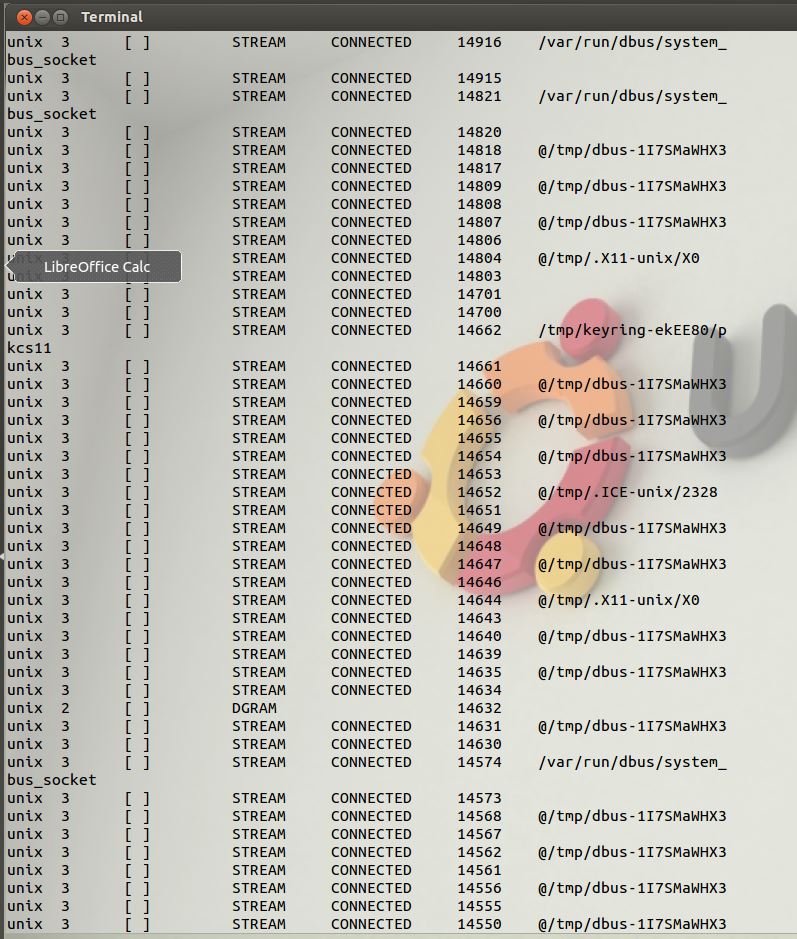
I tried to see if Victim was connected, and chose google as a ping target on a whim . . .

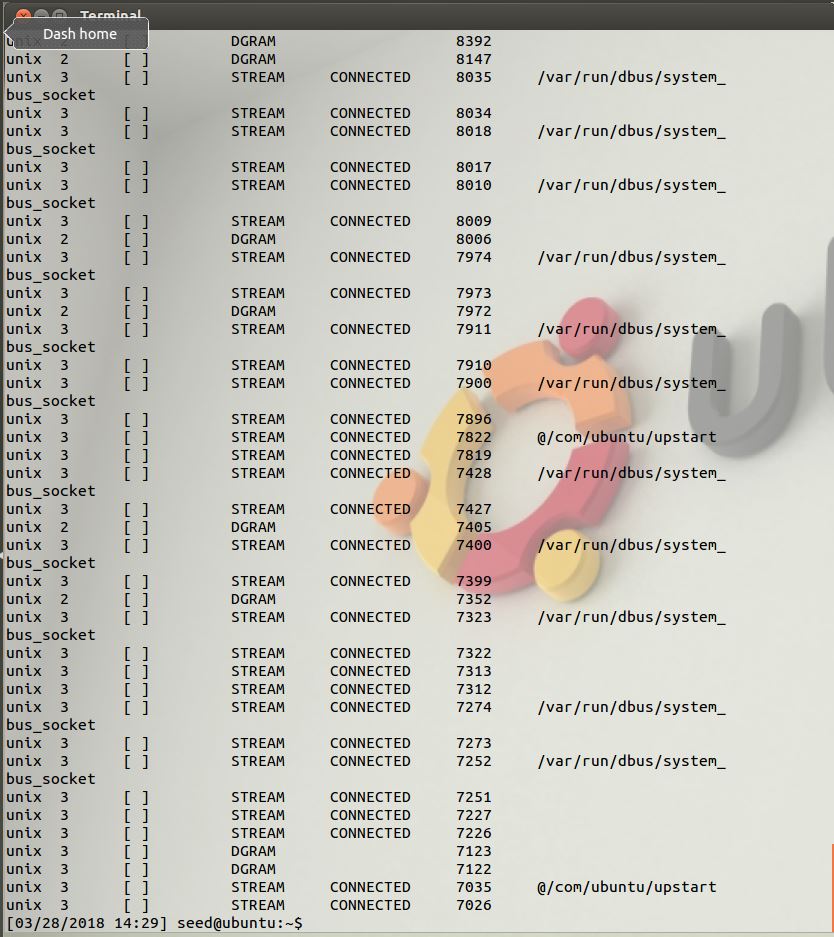


. . . which did not work. So maybe these VMs are restricted to the network within the hardware.

Starting to work through the project’s instructions, I tried to check the maximum size of the backlog on Victim, which produced no output. I do know why now, but I’ll explain that in chronological order.

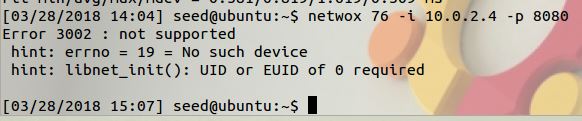


Fortunately, checking the actual status of the queue on Victim worked just fine:

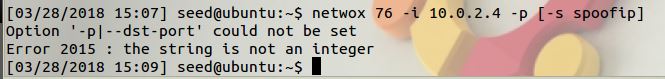


The instructions said to look for the status of ESTABLISHED, but I’m sure that CONNECTED here means the same thing, so all’s working fine in the queue.

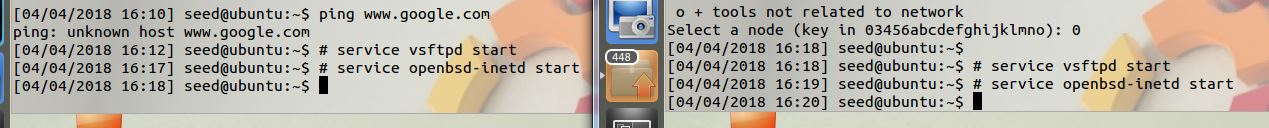
So the next bit is to get Attacker to start an SYN Flood (DOS attack) against Victim, which didn’t really work.



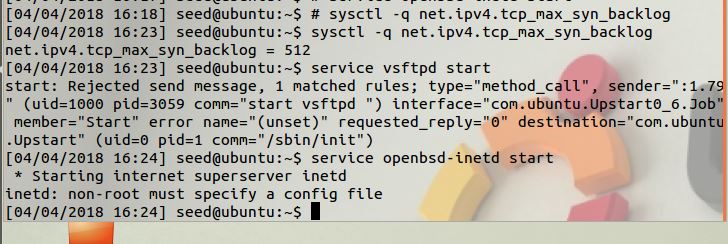
. . . or the second time . . .



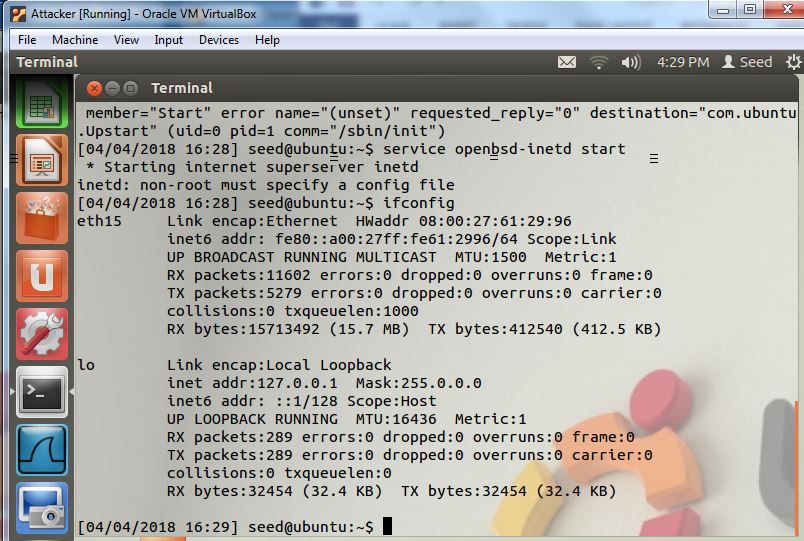
So not sure what’s wrong, I noticed the bits about starting the servers, which I hadn’t tried. I ran the commands on both Victim and Attacker, but they gave no output so I figured they might be working in the background.



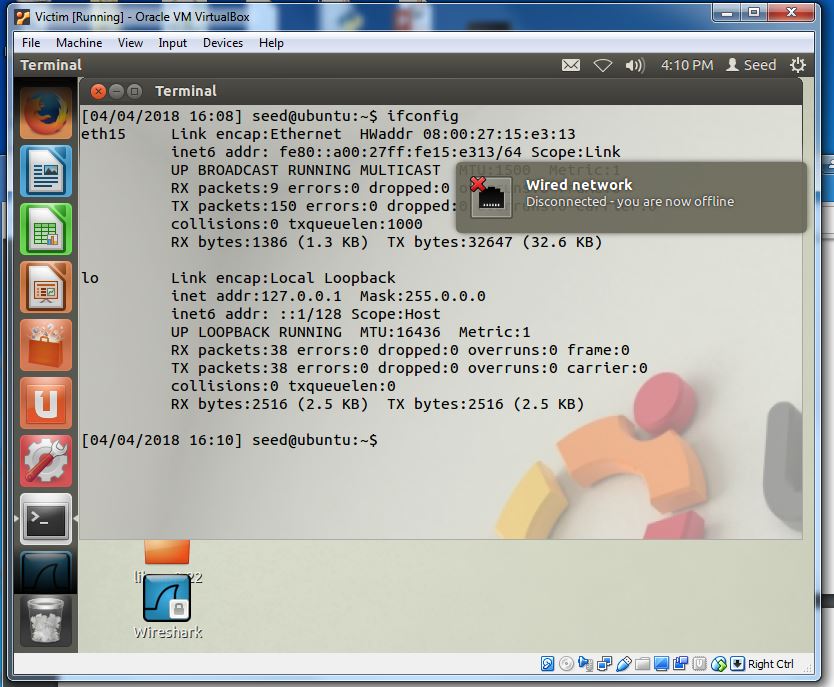
Turns out, the # isn’t part of the command, and if you leave it out, you get the following output:



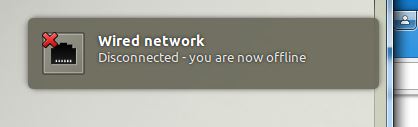
(this is Victim here)

After a bit of research online I decided to run ifconfig again, and Attacker seems to have forgotten its IP address.

Not sure how to get it back, I decided to call it a day and shut them all off.

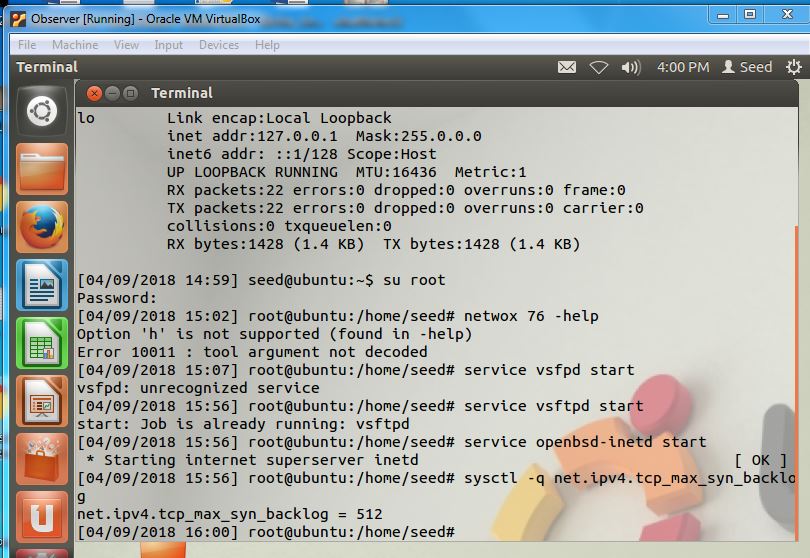
The next day I found the document about reinitializing the MAC addresses to solve connectivity issues.

After 3 cycles of off, refresh, reboot, ifconfig, I determined that too wasn’t working. (see above) It also started giving me that weird message there.

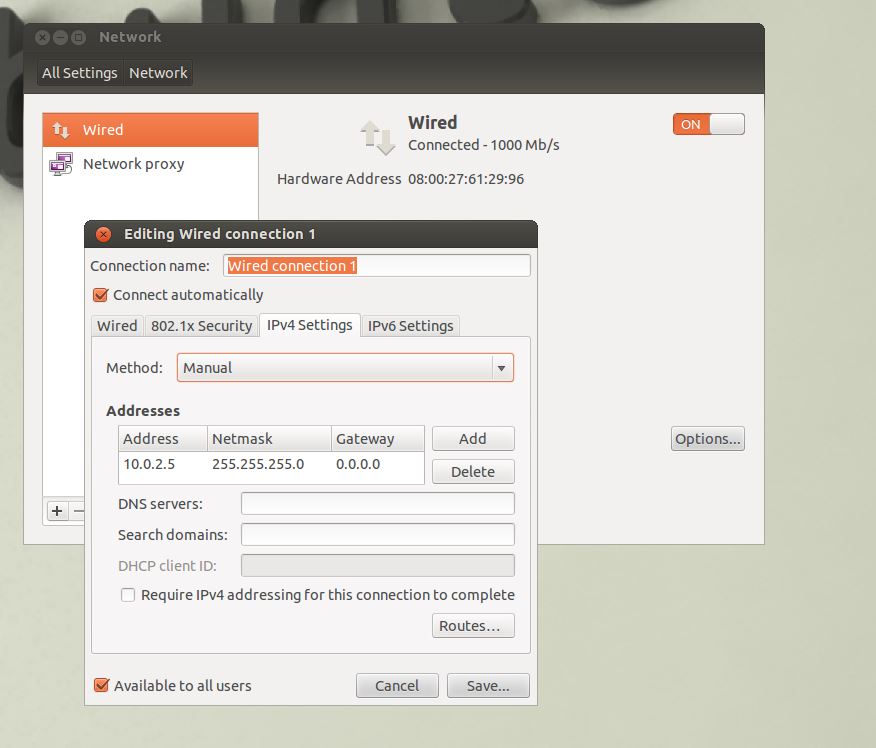


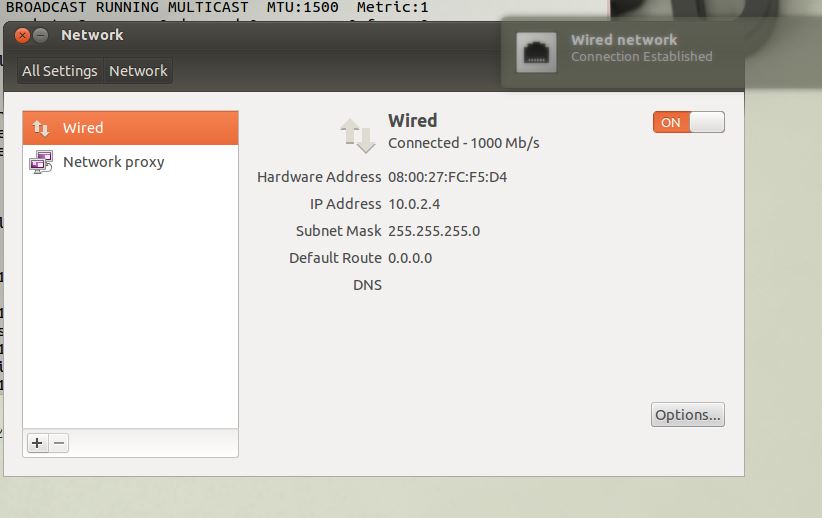
Ok, so, what wires? They don’t even need to leave the hardware to get to each other.

After several days of trying to refresh things and searching through the documents provided, and then getting help from the Professor, apparently I was in the user mode not the root mode, which is what those # meant earlier. Observer was the first to get into the new mode, and I started rerunning the commands:

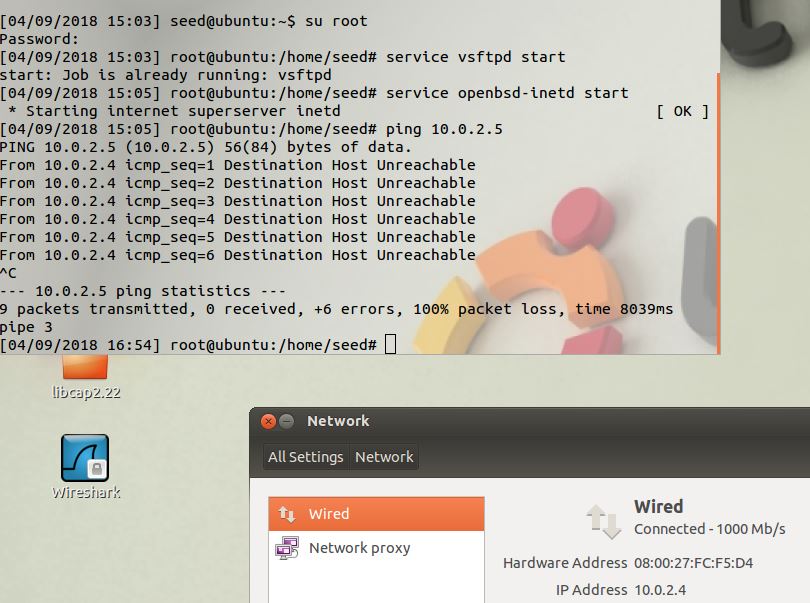


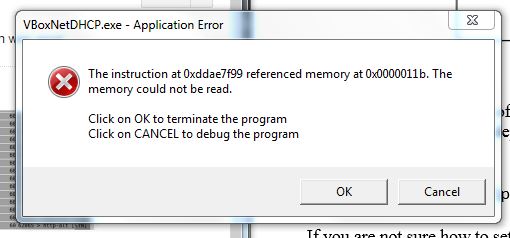
Then I attempted to force the connection by telling the network settings in the VM (Attacker went first), and it finally said connected! (reopened the settings window to show details)



After manually forcing Victim to connect too, . . .

. . . I had Victim ping Attacker, which failed.



Also I occasionally got this message:

. . . which I was later told means I had too many VMs open (I had a few clones running in case I needed another one to swap in) and that kinda ate up too many resources.

At this point I’m stuck again because they say connected but won’t ping each other or access the internet.