# Week 8 Homework submission

### **Phase 1**: "I'd like to Teach the World to *Ping*"

1. Run fping -g -r 1 <CIDR Range>
   1. The ranges that were scanned:
      1. 12.205.151.91/24
      2. 15.199.151.91/24
      3. 15.199.158.91/28
      4. 15.199.141.91/28
      5. 15.199.131.91/28
      6. 15.199.121.91/28
      7. 15.199.111.91/28
      8. 15.199.100.91/28
      9. 15.199.99.91/28
      10. 15.199.98.91/28
      11. 15.199.97.91/28
      12. 15.199.96.91/28
      13. 15.199.95.91/28
      14. 15.199.94.91/28
      15. 11.199.158.91/28
      16. 167.172.144.11/32
      17. 11.199.141.91/28
      18. 11.199.131.91/28
      19. 11.199.121.91/29
      20. 11.199.111.91/28
      21. 11.199.100.91/32
      22. 11.199.99.91/24
      23. 11.199.98.91/28
2. Found 12.205.151.1 and 167.172.144.11 alive
3. All ICMP requests are at layer 3

### **Phase 2**: "Some *Syn* for Nothin`"

1. Run nmap -sS <ip address to scan>
2. Results for 12.205.151.1 and 167.172.144.11 alive
   1. 12.205.151.1 no default ports open from 1-1000
   2. 167.172.144.11 port 22 is open to the public. This allows ssh access.
3. Syn scans are handled on layer 4

### Phase 3: "I Feel a *DNS* Change Comin' On"

1. The hosts file under /etc has been modified
2. Rollingstone.com is pointed to 98.137.246.8
3. 98.137.246.8 resolves to unknown.yahoo.com
4. DNS occurs on layer 7

### Phase 4: "Sh*ARP* Dressed Man"

1. The packet capture note is in the /etc folder. The file name was packetcaptureinfo.txt
2. It routed to [secretlogs.pcapng - Google Drive](https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view)
3. The hackers source address is 10.0.2.15
4. The hacker was trying to get to www.gottheblues.yolasite.com
5. The hacker was attempting to do an arp scan of the network
6. http is on layer 7 and arp is on layer 3