Man in the middle

All of the following will require at least 2 machines:

- A machine to run ettercap from. I used Kali.
- Some other machine (windows or linux)
- Make sure the machines can ping each other. You can type `ip a` to view your ip addresses. Make sure they can both ping out of the network. They should be in the same subnet.

To launch a mitm attack, you will most likely want to use `ettercap`. A simple ettercap run is shown as follows:

```
    ettercap -T -q -i eth0 -M arp /// ///
```

You can view the manpage to view what the options are above. (-M means mitm, arp means arp poisoning, the triple slashes represent the entire LAN). As it is running, you can hit the `h` key for some inline help. It will allow you to activate/deactivate plugins, other stuff, and end the attack.

You should try it and verify that the gateway mac address on your victim machines have changed to correspond to the mac address of your Kali machine.

Part I

Begin by doing a mitm rewrite select dns as shows in this video. You can edit `/etc/ettercap/etter.dns` to decide how to intercept traffic. You should make it so anytime the victim tries to access `www.nfl.com` they will be redirected to the website for `submit.computing.utahtech.edu`. Take a screenshot that proves this from your victim.

Hint: you could also add the `-P dns_spoof` flag to the above ettercap command.

Part II - Exploration

For this part, you can choose on of the following:

- Figure out how to use one other filter or plugin. Take a screenshot of how you used it. Write a short paragraph on what it does.
- Research man in the middle attacks. Can you find any examples of real-life attacks where hackers used this method? Write a short paragraph on it.

Submit

A single pdf document is great.