# Man in the middle

All of the following will require at least 2 machines:

- Your kali instance
- A victim machine (linux or windows)

To launch a mitm attack, you will most likely want to use [ettercap](https://www ettercap.org) found in kali. There is a GUI utility, but I had more luck with the CLI interface. A simple ettercap run is shown as follows:

```bash
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 double 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 using your kali machine to force all traffic to be routed through it and rewrite select dns as I demoed in class. 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](https://www.nfl.com) they will be redirected to the website for [submit.cs.dixie.edu](http://submit.cs.dixie.edu). Take a screenshot that proves this from your windows victim.

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

## Part II - Modify FTP

- From the victim, make sure you can still create an ftp connection to 144.38.193.202. (You should have written down usernames/passwords in an earlier assignment, but we don’t really need them. Pay attention to the banner that the server sends back)

- From kali: We want to rewrite the ftp prompt to something else:
  - create a filter in `/usr/share/ettercap/`, maybe named `etter.filter.ftp` with the following contents. (If you copy and paste, it might not work correctly)

    ```python
    if (tcp.src == 21 && search(DATA.data, "ProFTPD")){
        replace("ProFTPD", "NUGS000");
    }
    ```

  - Compile the filter

    ```
    etterfilter name_of_filter -o name_of_compilation
    ```

  - Fire up ettercap and load that filter (You can look at ettercap manpage, but it is essentially adding the flag `-F path_to_compiled_filter`.

  - See what happens when you FTP from the victim again. You are hoping to see the earlier banner message replace the string of `ProFTPD` with `NUGS000`, or whatever string you put above. Take a screenshot.

## Part III - Exploration

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.