Man in the middle

All of the following will require at least 2 machines:

- A machine to run ettercap from. I used my ubuntu instance as Kali wouldn’t cooperate. Install \texttt{ettercap-text-only}. Enable 2 network adapters. The first should be a \texttt{nat-network}. The second should be \texttt{bridged}. Click on advanced on the second one and \texttt{Allow all} packets in promiscuous mode. (Run ettercap from this machine)
- Your kali machine (One interface connected to the nat network). I am using this machine as the victim.
- Make sure they can ping each other over the host-only network. You can type \texttt{ip a} to view your ip addresses. If the ubuntu machine is not getting a second ip address, edit \texttt{[/etc/network/interfaces]} and add another 2 lines for \texttt{eth1} (they look the same as the lines that have \texttt{eth0}). Don’t delete any lines)
  (Reboot)

(I also had success putting attaching both machines to a single nat network)

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

\begin{verbatim}
ettercap -T -q -i eth0 -M arp ///</ ///</\end{verbatim}

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 \texttt{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 ubuntu machine to force all traffic to be routed through it and rewrite select dns as I demoed in class. You can edit \texttt{[/etc/ettercap/etter.dns]} to decide how to intercept traffic. You should make it so anytime the victim tries to access \texttt{www.nfl.com} they will be redirected to the website for \texttt{submit.cs.dixie.edu}. Take a screenshot that proves this from your victim.

Hint: you can add the \texttt{-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.