ECE 478 / CS 419: **Network Security**
Homework 5: due Friday June 6

Instructions:

- Submit typed solutions, following the rules in the syllabus.
- Include the "disclaimer" given in the syllabus!

Overview

This homework will take place on the DeterLab system, a controlled environment where you can safely wreak havoc. It is a bit of a pain but worth it for the kinds of malicious things I want to ask you to do.

Setting up

You should receive an email setting up your DeterLab login information. Follow the instructions there to get the account ready. Then, to get everything ready for the assignment:

- Log into DeterLab at https://www.isi.deterlab.net/index.php3.
- From the `Experimentation` menu on top, select `Begin an experiment`.
- Name your experiment `mitm-YOURNAME` – it has to be unique among all students.
- Put the following as the NS file: `/share/education/MITM_UCLA/mitm.ns`
- Set "Idle swap" to 1 and "Max Duration" to 6.
- Submit and wait.

Loading the experiment

In your main DeterLab account screen you should see a list of "Current experiments" containing your experiment. Click on the name you gave it to see more information.

To actually work on the experiment, it has to be "swapped in" — that is, physically loaded on some virtual machine somewhere. It will timeout after a certain amount of time, so you may have to swap in several times. If you are a good citizen, you will swap out your experiment when you are not using it (since DeterLab is a shared service with limited resources).

You can swap an experiment in/out with the links in the yellow box to the left of the screen. **Don't use** the "Terminate Experiment" option — that will clobber everything.

For more information: https://education.deterlab.net/DETERintro/DETERintro.html

Connecting to the experiment

This particular experiment sets up three nodes called `alice`, `bob`, and `eve`.

These nodes are not directly accessible from the Internet. You have to take two hops to reach them.

- Connect via ssh to `USERNAME@users.isi.deterlab.net`, and login with your DeterLab password.
- From there, ssh to `NODENAME.mitm-YOURNAME.osunetsec.isi.deterlab.net`, where `NODENAME` is either `alice`, `bob`, or `eve`, and `mitm-YOURNAME` is the name you gave the experiment previously.
- Since you only have shell access on the experiment nodes, it may be useful to use SSH-tunneling so you can use your local web browser. More information (including how to do it in PuTTY) is available at the link below. But for reference:

  ```
  ssh username@users.isi.deterlab.net -L \
      8888:alice.mitm-YOURNAME.osunetsec.isi.deterlab.net:80
  ```

  will map local port 8888 to port 80 on `alice`, so that browsing to http://localhost:8888 will connect to port 80 on `alice`.
- Your home directory `/users/osu478xx` is available on both the external `users.isi.deterlab.net` server as well as the experiment nodes. You can use this to transfer files in and out to your local machine.

For more information: https://education.deterlab.net/DETERintro/ssh.html

The actual assignment

I'd like you to do the activities described in https://education.deterlab.net/file.php/12/MITM_UCLA/Exercise.html. You will find the actual description of the activities under "Tasks", about 75% down the page.

Note that there is very little guidance given in the description of the tasks. I support this — it means that **you are expected to read** the first 75% of that assignment webpage, and also consult external reference material as well. The point is to learn how to use these tools.

Answer the questions given in the list of tasks, providing screenshots / commands to show your work.

Below are some additional tips for getting things done:

1. Eavesdropping Connect to `eve` via SSH. Use `ettercap` as described to snoop on the network. I found the terminal interface to `ettercap` slightly tricky — use the Tab key to get back to the menu if your cursor is stuck down below.

While `ettercap` is sniffing, use `tcpdump` (in another SSH session probably) to capture traffic. Use `chaosreader` along with the text-based `elinks` web browser to inspect the captured traffic (or transfer the pcap file and use a local instance of `wireshark`). Or as another alternative, you can directly inspect the traffic in `ettercap`.

2. Replay attack You'll probably want to use the SSH forwarding trick described above, to interface with the web stock ticker.

3. Insertion attack Write an appropriate filter, compile it with `etterfilter`, and load it into `ettercap`.

To verify that it works, you should cause `alice` or `bob` to view the stock ticker website as a user.

4. MITM should be relatively self-explanitory.