Programming assignment #1

CprE 430/530 Due Tuesday Oct 9

This assignment focuses on installing and running the netdump program.

You will use your KALI machine inside of ISELab. (See 530 lab instructions on how to access and configure your KALI machine)

Do the following steps from your KALI box

1. Download the source code for the program netdump. You will find the source code spock.ee.iastate.edu. From a terminal window in your KALI machine
    a. Type 'mkdir netdump'
    b. Type 'cd netdump'
    c. Type wget spock.ee.iastate.edu/netdump.tar
    d. Type 'tar –xvf netdump.tar'

2. Build the program netdump

    a. The code was written for a FreeBSD UNIX: to get it to run on Linux or Debian machine edit netdump.c and make this change:

```
extern void bpf_dump(struct bpf_program *, int); <-- Old
extern void bpf_dump(const struct bpf_program *, int); <-- New
```

    b. Install libpcap-dev. To do this: Type: sudo apt-get install libpcap-dev

    c. To compile the program type 'make' in the netdump directory

        GCC 4.9 builds without any warnings. GCC 5.3.1 raises warnings over functions `error` and `warning` as implicit declarations but runs fine otherwise.

3. To run the program type sudo ./netdump. To stop the program type control-C

    You will see blocks of HEX numbers scrolling across the screen.

To turn in: Run the program and then type control-C. Turn in a printout of a sample trace and tell me what type of packets each one is based on the Ethernet type/Len field.

NOTES:

For C and UNIX help see: http://www.dougj.net/modules/index.html

I have setup a slack channel inside the 530 slack team where you can talk with each other the programming assignments.