# COMS 4180 Network Security Written Assignment 4

**Due Tues, April 20, 2016, 10:00pm** Eastern time.
50 points
The homework is to be done individually.
The papers for questions 2,3,4 are under the Lecture 11 module.
NO LATE HOMEWORK WILL BE ACCEPTED. The answers will be given in class on the 22nd, which is the last lecture before the exam.

**What to submit:** A text/pdf/word file with your answers. Submit via canvas.

**1. 15 points (10 for part a, 5 for part b)**

Scenario: there is a Linux system on which runs a set number of processes performing some task. The server is up 24 x 7. The only user on the system is the administrator, who logs in as root periodically to perform routine checks and maintenance.

a, Using only the data available from the netstat and top commands, describe how an IDS can monitor the Linux system for suspicious connections and usage. Include how often to collect data, what data (from that produced by netstat and top) to use and what statistics to compute. Also discuss the likeliness of false positives and false negatives.

b. Suppose the developers of the software running on the system are given logins to the system. How would this impact the IDS collection and analysis of the data and how may it impact the accuracy of the results?

**2. 10 points**

Using the ZigBee-Exploited-wp.pdf and article (link below from the assigned readings in Lecture 11), what security issues were identified in ZigBee?

http://www.networkworld.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html

**3. 10 points**

In the paper oakland2013-peekaboo.pdf *Peek-a-boo I See You: Why Efficient Traffic Analysis Countermeasures Fail*, what are the authors able to identify (what is it that a client receives can be identified) via traffic analysis? Do any of the countermeasures they discuss prevent the identification? For each countermeasure they tested, briefly describe (1 to 3 sentences) how they are able to thwart the countermeasures or how the countermeasure prevents the identification. For example, if they are able to thwart the countermeasure, what in the traffic were they able to measure to perform the identification.

**4. 5 points** (points for each part are all or nothing, no partial credit)

In wright06a.pdf:

a. (1 point) What transport layer protocol was used in the traffic the authors analyzed?

b. (2 points) +What three features from each packet did the authors use in their analysis?

c. (2 points) What were the 8 applications for which they collected traffic?

**5. 10 points** (5 points for each example)

Find 2 examples of IoT devices (includes cars) being exploited/hacked in the past 2 years and explain what the issue was with each that allowed it to be exploited/hacked. You may not use the dam in NY state as one of the examples. You may not use a malfunction due to a bug in the software if there was no exploit of the bug. For example, the NEST thermostat bug from early 2016 was a malfunction due entirely to the bug and not a malicious act.