**CEG4430/6430 Homework 4**

(30 Points)

1. Please read the attached paper for “0x20” and answer the following questions based on the given parameter.

* α = the number of different DNS IDs
* β = the number of source ports
* ϒ = the number of source ports excluded (e.g., 1024)
* θ = the number of authority servers
* l = the length of a domain (number of letters)
  1. What is the probability for a DNS poisoning attack to be successful without 0x20? (5 Points)
  2. What is the probability for a DNS poisoning attack to be successful if 0x20 is deployed? (5 Points)

1. Attackers may be actively attempting to evade a detection system. We assume that a student has developed a webserver that listens on TCP port 80. However, this webserver is vulnerable to an attack. If an HTTP request contains a string of “ATTACK” (case sensitive), the webserver will be exploited. An example is illustrated as follows:

|  |  |  |
| --- | --- | --- |
| IP Header | TCP Header | GET ATTACK http://www.google.com/ |

You have designed a signature-based (a.k.a., misuse) intrusion detection system, which will raise an alert if it finds “ATTACK” in *one* TCP packet.

* 1. How can an attacker successfully launch attacks while evading your detection system? (5 Points)
  2. How can you modify your detection algorithm to counteract? (10 Points)

1. Collecting benign samples to train a model for anomaly detection is usually very expensive. Let us assume Alice and Bob accomplish the identical detection rates and false positive rates. The following figure plots how the size (e.g., memory consumption) of the model (y-axis, used to profile the benign behaviors) grows as we use more benign samples (x-axis) to train the model. Which system do you prefer according to the figure? **Give two reasons**. (dotted-Alice, line-Bob) (5 Points)

Alice

Bob