CS5434 – Homework 4

Due Tuesday November 12th, 2013.

Problem 1

Consider the description of Blackhole v2 at http://blog.spiderlabs.com/2012/09/blackhole-exploit-kit-v2.html with a particular focus on the initial obfuscated javascript described there. Develop one or more snort signatures to detect this javascript. Now run snort with your new rule(s) against your background pcaps of your own traffic (from homeworks 2/3) and refine them to avoid false positives on that traffic.

Do you think this is a good strategy to detect Blackhole exploit attempts. Why or why not?

Problem 2

Suppose we wish to send the string "Signature" at the beginning of a TCP connection, but as three IP fragments: the first containing "Signify" as bytes 0-6, the second as "atu" as bytes 4-6, and the last being "re" as bytes 7-8.

Work out the ip identification and fragment offset fields, the ip length, and the (relative) tcp sequence numbers of all three packets.

Problem 3

Take the heapspray code from http://www.thegreycorner.com/2010/01/heap-spray-exploit-tutorial-internet.html and get it to work in your browser (eg by loading an HTML file from disk). Note, not the exploit itself (which is very unlikely to work in a current browser) just the heapspray with enough initialization code to get it to run. Now vary the number of iterations in the main for() loop, and measure the size of the browser as a function of this loop count (eg using ps on a unix/Linux system) over a wide range of values. Can you determine the increments in which the browser gets memory from the OS? How much overhead is there between successive copies of the nop-sled/payload combination?