CS 5434 Assignment 3

Due via CMS on Tuesday Oct 22nd by 11:59pm

Problem 1

Consider a worm attempting to spread stealthily on an internal class B network via the following strategy. It makes scanning probes once per hour. 90% of the time, it picks a random address on the same class C network as the currently infected machine. 10% of the time, it picks a random address from anywhere in the class B.

Assume that 5% of addresses are vulnerable (all with equal likelihood). Assume also that there are filters that control access in and out of each of the class C subnets and all the others. The filters attempt to block scanning. There are no filters controlling access within each class C subnet.

a) Should the filter focus on blocking inbound or outbound probes?

b) What is the maximum average number of probes per infected IP that the filters can allow through, before blocking, in order that they contain the worm below the epidemic threshold?

Problem 2

Consider a network intrusion detection system that produces one false positive alert per million packets, on average. Consider this system deployed on a 1Gbps link, which is on average 50% utilized. Assume that average packet size is 500 bytes including all preamble/postamble.

a) How many false positives per week must the security operations team investigate?

b) If it's only permissible for the IDS to produce one false report per day, how many packets must go past per false report?

Problem 3

Consider a DDOS botnet that is controlled in the following manner. Each bot makes HTTP connections on port 80 to the command and control server (thus likely evading firewall rules at many sites). The command and control server responds with a plain text file containing lines of the following form

<pkt-type> <ip>/<net>[:<port>] <rate> <duration>

Here <pkt-type> is one of ‘SYN’, ‘ICMP’, ‘GET’, ‘DNS’, <ip>/<net> is a specification of an address range to flood, the destination <port> number is optional, and <rate> is the number of packets to flood per second to random destinations in the target range for <duration> seconds. The command language allows for multiple lines per file, with the bot carrying out all of them simultaneously (infected machine bandwidth permitting).

Write a snort rule, or set of rules, to identify these commands on the wire. Consider how to reduce false positives against the terms in this command language occurring naturally in web documents.

Problem 4

In HW2 you gathered a sample of your own machine traffic for 12 hours. Taking that sample (or a new one), analyze the address ranges and ports occurring in it. For example, you could use tcpdump, cut, grep, sort, and uniq on the Unix/Linux command line, or some other tools of your choice. Based on your analysis, construct a set of firewall rules that would allow all the traffic in your sample, while allowing as little other traffic as practical.

For syntactic definiteness, use the rule syntax of pf as at

http://www.openbsd.org/faq/pf/filter.html

Provide enough detail of your analysis of your traffic that the TA can assess the correctness of your rules.