Worksheet 4: Monitoring
15.05.2012, Garching

1 Monitor Setup and Configuration

Configure a monitor using a virtual machine on your lab PC. This monitor should include, at least:

a) Snort 2.9+ (from source, see [http://www.snort.org](http://www.snort.org))
b) barnyard2 (from source, see [https://github.com/firnsy/barnyard2](https://github.com/firnsy/barnyard2))
c) MySQL

We urge you to use Debian 6. If you insist on using another distribution, you are on your own.

Going through the tutorial at [http://www.snort.org/assets/167/IDS_deb_snort_howto.pdf](http://www.snort.org/assets/167/IDS_deb_snort_howto.pdf) may be helpful for you. Do not blindly go through the tutorial, it sets up more than you need, but take from it what you need.

2 Custom Rules (graded)

Snort is a powerful IDS/IPS and allows one to write custom rules. Consider the following scenarios and write custom rules to address the given problems. We will test these in class using the extra NICs on each lab workstation and grade you based on the results. Be sure that your setup works in the Lab!

2.1 Shellcode

Write a single rule that will match on the three patterns listed below anywhere in the packet. Note the similarities and write your rule such that it will match on similar content not presented.

a) 0x1A 0xBC
b) 0x1A 0xAB 0x4C
c) 0x1A 0xB3 0xFC

2.2 Search Engine Searches

Write a rule that will hit whenever a user searches either google, bing, or yahoo (all top-level domains) for the keywords “malware”, “rootkit”, and/or any search for IP addresses that we use in our honeynet.