Snort: Supplement

Exercises

1. A production Snort sensor should regularly update its rule set. Install PulledPork (<https://code.google.com/p/pulledpork/>), which is a tool to automate the download of Snort rules.
2. A more realistic intrusion detection system might have two network cards- one to act as a sensor, and a second to provide a management interface. Build such a system.
3. Another approach to detecting ARP spoofing attacks is to use the tool Arpwatch. Test it and compare it to Snort.
4. There are other output modules besides those included in the default snort.conf file. Configure Snort to output its alerts to a comma separated value (.csv) file.
5. Configure a Snort sensor that logs to a remote MySQL database using Barnyard2, available from <https://github.com/firnsy/barnyard2>.