PulledPork

JJ Cummings

PulledPork

- What is it?
- Why build it?

Getting Started

- Requirements
  - Snort
    - With proper configuration (so_rules)
    - http://vrt-sourcefire.blogspot.com/2009/01/using-vrt-certified-shared-object-rules.html
  - Perl
  - Permissions
  - Free Space
  - Oinkcode

The Environment

- FreeBSD 7.2 Release i386
  - Minimal Install
  - Perl 5.10
    - LWP::Simple
- Snort 2.8.4.1
  - Configured for use with dynamic rules

The Setup

- Latest pulledpork
- Config files
  - /usr/local/etc/snort/pulledpork.conf
  - /usr/local/etc/snort/disablesid.conf
- Runtime options
  - -c <path>, -i <path>, -T, -H, -n, (-THn)
  - Many others, see -help or README

The Beef

- Demo in VM as noted in The Environment slide

Questions / Comments

- Project Page => http://code.google.com/p/pulledpork
  - Suggestions
  - Bugs
  - Comments
- Google Group => http://groups.google.com/group/pulledpork-users
  - Suggestions
  - Bugs
  - Comments