Performance Tuning Snort

Steve Sturges

SOURCEfire®

Agenda

- Goals of Performance Tuning Snort
- Techniques
  - Perfmon Preprocessor
  - Preprocessor Profiling
  - Rule Profiling
- White paper
- Q&A

Goals of Performance Tuning

- Improve Snort throughput
  - Higher MB/s
  - Inspect traffic more efficiently
- Reduce Packet Latency
  - Important when inline
  - Lower per packet processing time
  - Eliminate network hiccups

Perfmon Preprocessor

- Configuring Perfmon
  - Printing to Console vs File
    - File provides quicker output, but need to post-process CSV file
  - Packet Count, Time Intervals, Exit Only
  - Looking at Flow Data
    - Breakdown of port and packet size distributions
    - Look for High Port to High Port traffic
    - Look for Heavy talkers/listeners

Perfmon Preprocessor (cont)

- Stats Categories
  - Throughput
  - CPU Usage
  - Pattern Matching
  - Stream
  - Frag
- Looking at Flow Data
  - Breakdown of port and packet size distributions
  - Look for High Port to High Port traffic
  - Look for Heavy talkers/listeners

Perfmon Preprocessor (cont)

- Throughput Stats
  - Higher = better performance
  - Increase by steps throughout
- CPU Usage
  - Lower = better performance
  - Decrease by steps throughout

Perfmon Preprocessor (cont)

- Pattern Matching Stats
  - Lower = better performance
  - Decrease by eliminating benign traffic from inspection
    - Reduce number of TCP reassembled packets
    - Reduce HTTP client & server flow depths
    - Limit size of DCE/RPC reassembled packets
    - Ignore encrypted traffic
    - Ignore FTP data channel transfers
    - BPFs & Ignore Ports

Perfmon Preprocessor (cont)

- Stream Stats
  - Cache Faults, Timeouts
    - Increase number of sessions tracked
    - Increase memcap
    - Correctly set timeout
  - TCP SYNs vs SYN/ACKs
    - Snort performs best when seeing symmetric traffic
- Frag Stats
  - Frag Faults, Frag Auto Deletes, Frag Timeouts
    - Increase max_frags and memcap
    - Use prealloc_memcap or prealloc_frags
    - Correctly set timeout

Perfmon Preprocessor (cont)

- Flow Data
  - Breakdown of port and packet size distributions
    - Reduce number of packets included in TCP Reassembly
  - Look for High Port to High Port traffic
  - Look for Heavy talkers/listeners

Preprocessor Profiling

- Performance Breakdown of Snort's Phases
  - Preprocessors
    - Sub categories
  - Detection
    - Pattern Matching (MPSE)
    - Rule Options (various option types)
  - Output/Event Logging

Preprocessor Profiling (cont)

- Checks
  - Reduce to improve performance
    - Correctly configure preprocessor ports
    - Ignore traffic as noted earlier
- Average per Check
  - Reduce to improve performance
    - Eliminate large blocks of data, correct configuration of TCP reassembly ports/services
    - Eliminate unnecessary preprocessors based on rule set
    - Eliminate unnecessary rules to help MPSE
    - Use faster pattern matching algorithm

Rule Profiling

- Performance Breakdown of Individual Rules
  - Rules as part of Snort's total time
  - Overlap across rules with common detection options
    - For rules within same group, place common options first and in same order
    - Start with flow:established,<direction>

Rule Profiling (cont)

- Microseconds
  - Reduce to improve individual rule performance
    - Rule time vs Total Snort time
    - Investigate if ratio is > 5% total
- Checks vs Matches vs Alerts
  - Can rules that are not matching be turned off?
  - flowbits:noalert can result in match but no alert
  - Reduce checks by improving uniqueness and accuracy of content option used for pattern matching
    - Should have at least one content in rule
    - Longest pattern used
    - Can specify alternate pattern with fastpattern modifier to content

Rule Profiling (cont)

- Average per Check
  - Most often caused by expensive PCRE
    - Reduce complexity of pattern
    - Reduce possibility of recursion

      Split into multiple rules in cases of many “ORs”
    - Use config options to restrict impact of PCRE

      pcre_match_limit

      pcre_match_limit_recursion

Tuning Guidelines Document

- Posted on Snort.org
  - http://www.snort.org/docs/development-papers/
- Rule Writing Specifics
  - VRT White Papers
    - Rule Writing Methodology
  - VRT Performance Rules Creation Series
    - Performance Rules Creation I
    - Performance Rules Creation II

Questions?

SOURCEfire®