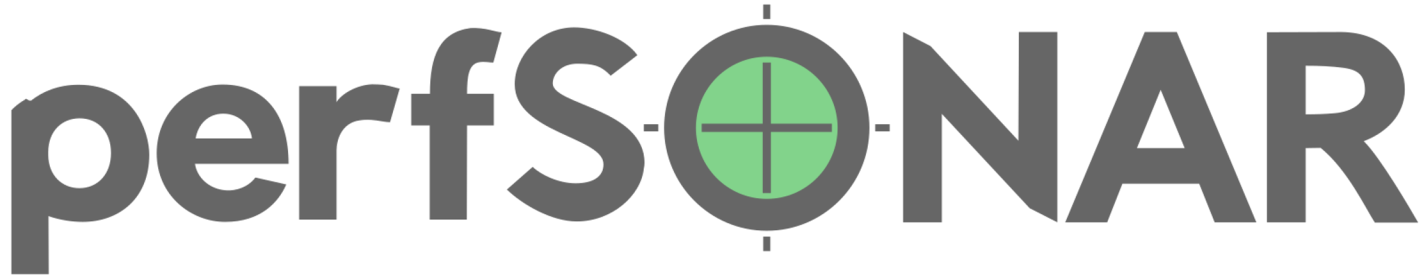


perfSecurity

The intersection of perfSONAR and Information Security

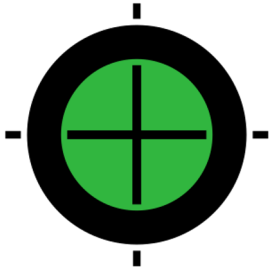
Mark Feit · Internet2 / The perfSONAR Development Team · mfeit@internet2.edu

Third European perfSONAR User Workshop · May, 2022

perfSONAR is developed by a partnership of

Agenda

- ~~Introduction to perfSONAR~~
- Infosec for perfSONAR
- perfSONAR for Infosec



InfoSec for perfSONAR

Security in perfSONAR and what your Information Security organization can add

General Security Stance

- Installation bundles install and run only necessary services
- Host firewall locked down to required ports
- Limited requirement for user accounts
- HTTPS required
  - Signed certificate not required
  - May make it configurable in a future release
- Regular review of allowed ciphers
- Security-related upgrades to applications (Automatic)
- Vulnerabilities patched in hours to days

pScheduler Terminology: Tasks and Runs

- A ***task*** is a job pScheduler is given to do:

  "Measure UDP throughput between this perfSONAR node and **`ps-sdmz.example.edu`** at up to 1 Gb/s for 30 seconds. Repeat it once per hour from now until next Tuesday at 4:15."

- A ***run*** is a single execution of the requested measurement.
  - All tasks have at least one.

pScheduler Terminology: Participant

- perfSONAR node actively participating in a measurement
- One Participant
  - Round-Trip Time – Ping can run on one end, other end is passive
  - Latency – OWAMP/TWAMP client runs one one end, other end runs a service but is otherwise passive
- Two Participants
  - Throughput – Requires a client and server, one on each end

pScheduler's Trust Model

- First ("lead") participant (All Tests)
  - Oversees the entire measurement process
  - Must trust the requester
  - Makes requests of other participants if there are any

- Other participants (**`throughput`** and others)
  - Must trust the lead participant
  - Transitive trust: other participants trust the requester if they trust the lead.

Access Controls: Who Do You Trust?

- All of pScheduler operates through a REST API
  - Command-line tools
  - pSConfig
  - Third-party applications
- API is mostly open
  - Certain operations restricted based on originator's IP or originator-provided key
- Information considered confidential is withheld on read
  - Designated in JSON by keys beginning with an underscore (e.g., **`_secret-thing`**)
  - Applied globally by the API so nothing slips out
- Testing regulated by the *limit system*.

Restricting Use: pScheduler's Limit System

- Determination of who is requesting that pScheduler run a task (*Identification* and *Classification*)
- Imposition of restrictions on those tasks (*Limits* and *Applications*)
- Application of changes to the task before making decisions (*Rewriting*)
- Assignment of priority to the task (*Prioritization*)
- Gory details in *Know Your Limits* on YouTube

Limit Configurations

- pScheduler – No limits by default
  - Anything goes

- Bundles – Sane defaults for untrusted requesters
  - Harmless tests allowed
  - UDP throughput restricted to 50 Mb/s
  - Resource- and schedule-intensive tasks duration-restricted

When are the Limits Evaluated?

- **Initial Task Submission**
  - Task specification
- **Run Scheduling**
  - Task specification
  - Proposed time and duration

Limit Input: What is Considered?

- Hints
  - IP of requesting host `198.151.100.207`
  - IP on server where request arrived `192.0.2.8`
  - Other information (e.g., authenticated user) as means are developed
- Measurement type and parameters `{ … JSON … }`
- Scheduling information (only when scheduling runs)
  - Proposed start time `2018-09-05T15:19:08-05:00`
  - Proposed duration `PT27S`

Identification: Who's Asking?

- Takes input from the hints
- Applies a condition based on the identifier's *type*
- Makes a declaration about the requester:
  - "This requester is on one of the campus networks"
  - "This requester is on a known-hostile network"
  - "This requester is not on a research and education network"

Types of Identifiers

- **`always`** – Evaluates true every time
- **`hint`** – Does text matching on hint values
- **`ip-cymru-bogon`** – Determines if the requester's IP is in Team Cymru's list of bogon and martian IP addresses
- **`ip-reverse-dns`** – Does text matching on the requester's FQDN, reverse-resolved from its IP

More Types of Identifiers

- **`localif`** – Determines if the requester's IP is bound to an interface on the local system
- **`local-subnet`** – Determines if the requester's IP is on a subnet to which a local interface is connected
- **`jq`** – Runs a jq script with the hints as input; returns a Boolean
- **`ip-cidr-list`** – Determines if the requester's IP falls within a provided list of addresses or CIDRs
- **`ip-cidr-list-url`** – Same, but downloads the list from an external source

`ip-cidr-list-url` Address List Format

IPv4 and IPv6 addresses and CIDRs separated by newlines:

```
# Comment (Ignored)
192.0.2.0/24
198.151.100.37
2001:0db8:1bad:cafe/64
2001:0db8:dead::beef
```

`ip-cidr-list-url` Parameters

- **`source`** URL for retrieving list
- **`transform`** jq transform script (optional)
- **`exclude`** IPs/CIDRs to ignore
- **`update`** How often to get a new copy
- **`retry`** How often to retry on failure
  - Last successfully-downloaded list used
- **`fail-state`** Identify or not with no list

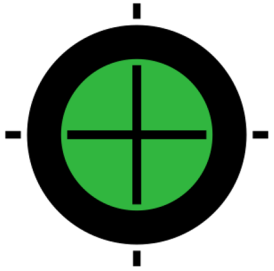
`ip-cidr-list-url` Applications

- Who do we like?
  - Campus and partner perfSONAR nodes
  - Registered researchers
- Who do we dislike?
  - Intruders detected by IDS
  - Published block lists
  - Anything else from your threat intelligence system

Advantage of this Model

- You publish your list(s)
  - Publisher can make decisions about who gets what list
- perfSONAR consumes it

- Decouples some administrative decisions from perfSONAR configuration
  - It's data rather than config
  - Set up perfSONAR's limits once: less maintenance



perfSONAR for InfoSec

What perfSONAR can do for your Information Security organization

Security as New Territory

- perfSONAR is typecast as a tool for network performance measurement.
  - We tend to sell it that way.
- Nothing in the current architecture precludes other applications.
- Let's stir some creative thought.

perfSONAR as a Unit Testing Platform

- We talk a lot about measurements in numeric terms
  - "How many Gb/s can we get between points *A* and *B*?"
  - "What is the path loss between points *A* and *B*?"

- Boolean measurements are still measurements
  - "Is host *H* reachable from {in,out}side?"
  - "Does the HTTP server serve page *P* to host *H*?"
  - "Does DNS answer external queries for internal-only hosts?"

perfSONAR as a Unit Testing Platform

- Run tests at regular intervals
- Post customized results to internal systems using archivers
  - HTTP(S) POST, RabbitMQ, Kafka, Syslog, SNMP Traps
  - No news is good news: drop results that show expected behavior
- pSConfig for central control
  - JSON configuration can be generated

True Stories: Open Ports

- A configuration containing a mistake was deployed
- SSH access was opened to a large swath of internal hosts
- Went unnoticed until other measures raised red flags
- Development is underway to do verification from an externally-deployed perfSONAR node.

What Can't perfSONAR Test?

- In theory? Not much.
- The measurements described earlier can be made with out-of-the-box perfSONAR.
- Anything else can be added with pScheduler plugins.

Plugins

- pScheduler offers pluggable extensibility:
  - New measurements — *Tests*
  - New programs to carry out the tests — *Tools*
  - New ways to dispose of results — *Archivers*

- Requirements:
  - A way to describe the test and its result
  - A program that can produce the result from the test, perhaps with some glue

- The development team is willing to adopt plugins of general interest and make them part of the perfSONAR distribution.

Non-Traditional Test Plugins: `netreach`

- Find out if any hosts on a network block are up
- Developed for use on SCinet
- Features:
  - Multiple scan methods (linear up/down, edges-in, random)
  - Limits on how many IPs to scan
  - Optional gateway vs. non-gateway check
- Simple yes/no result; not intended to be a network scanner.
- **`nmap`**-based tool plugin originally; replaced by **`fping`**.
- Not installed by default

Non-Traditional Networking: `openports`

- Find out if ports on host(s) are open
- Yes, this is a port scanner.

- Developed last year. Still needs some work.
- **`nmap`**-based tool plugin
- Not installed by default

Testing Topology

- Nodes inside the security perimeter can be used to test outbound.
- Nodes outside can be used to test inbound.
  - Use your existing nodes
  - Develop cooperative relationships with other institutions
  - “We’ll test yours if you’ll test ours”
  - Leverage pSConfig to minimize reconfiguration
- Add nodes where needed
  - Most security-related measurements require low-cost, low-spec hardware.
  - Some vendors implement perfSONAR on routers and switches.

Other Uses for Existing perfSONAR Tools

- Heartbeat
  - Run periodic tests that appear as intrusion attempts
  - Make sure protective infrastructure is producing alarms
- Filter Check
  - Attempt to retrieve blocked web sites
- Path Monitoring
  - Verify that traffic is taking an approved path through your infrastructure

Thanks!

- Questions or comments:
  - perfSONAR User List **perfsonar-user@internet2.edu**
  - Development Team **perfsonar-developer@internet2.edu**
  - Me **mfeit@internet2.edu**