perfSONAR

Node Maintenance: Security & Operational Concerns

ASTRON perfSONAR training

Antoine Delvaux, PSNC, antoine.delvaux@man.poznan.pl
Szymon Trocha, szymon.trocha@man.poznan.pl
24-26 September 2018

ESnet ENERGY SCIENCES NETWORK GÉANT INDIANA UNIVERSITY INTERNET2 UNIVERSITY OF MICHIGAN

Outline

- Introduction & Overview
- Security
  - Software Updates & Accounting
  - User Accounts & Machine Access
  - Physical Security
  - Service Audit
  - Firewalls & IDSs
  - Logging
- Conclusions

Introduction

- The perfSONAR Toolkit should be treated the same as any other host in your infrastructure
  - E.g. it should receive the same care and attention from the server team as something like the mail or DNS server
  - Those that forgot they had one are at risk for compromise, and may be upset about such an experience
  - There are many tools out there that can ease the burden, there is no replacement for a human regularly checking

MISS WORMWOOD?
YES, CALVIN?
YOU CAN PRESENT THE MATERIAL, BUT YOU CAN'T MAKE ME CARE.
RUMOR HAS IT SHE'S UP TO TWO PACKS A DAY, UNFILTERED.

Introduction

- Recommendations for deployment often mean allowing this resource to live in the cold dark internet, to allow for a clean view of pure network performance
  - This doesn’t mean we don’t want to forget about security or maintenance – in fact we need to be careful to implement adequate, intelligent, and performance focused countermeasures where we can
- The following sections outline some of the items that should be examined on a semi-regular basis.
  - N.B. All of these are ‘typical’ recommendations that are SOP for Linux servers, apply this knowledge elsewhere if need be.
  - Some are specific to perfSONAR

perfSONAR Risk

- Since perfSONAR hosts are usually fast, well connected hosts, the main risk is that someone will get on and use the host for a DDOS attack
  - If this happens, WE ALL SUFFER!
  - perfSONAR nodes will get taken down, making the perfSONAR ecosystem less useful
- Data on the host is not particularly valuable.

Security

Outline

- Introduction & Overview
- Security
  - Firewalls & IDSs
  - Logging
  - Software Updates & Accounting
  - User Accounts & Machine Access
  - Physical Security
  - Service Audit
- Conclusions

Firewalls

- Firewalls* have a role in the enterprise network
  - They protect against the unknown – they are designed to protect the network from bad things getting in, and private things from getting out.
  - *IF* you have scientific resources behind a firewall (e.g. you aren't using the Science DMZ paradigm yet) should you also place a perfSONAR host behind a firewall
    - This will give the perfSONAR host the same 'view' of what is going on
    - If performance is bad, you may want to consider a comparison with a perfSONAR host directly outside of the firewall, and testing to the same things.

*http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Access Control Lists (ACLs)

- You can use router or host ACLs to control who can run tests to/from your perfSONAR host
  - This can be used to reduce the DDOS risk
  - BUT: restricting access makes your host less useful! (for you, and others)
  - Detecting the DDOS using via traffic monitoring or an Intrusion Detection System is a much better solution
- The perfSONAR Toolkit features IPTables rules for all essential services – this can be considered a host-based firewall
  - More information here: http://www.perfsonar.net/deploy/security-considerations/
  - The administrator has the ability to add/delete rules, see the documentation link above for more details

Intrusion Detection

- There are numerous solutions in the IDS space (host based, appliance based, external server based).
  - All have positives and negatives
  - Typically the use of external systems should start as a conversation between you and your security people.
  - Host based IDSs are software packages that can be installed on the perfSONAR node – we will talk about some here.
- The perfSONAR toolkit comes with Fail2ban (http://www.fail2ban.org/wiki/index.php/Main_Page)
  - This software is designed to parse logs (apache, ssh access, etc.) and look for behavior consistent with attack vectors.
  - For example, a brute force SSH attempt from a host will result in several log messages in the secure log – fail2ban can detect this
  - When it finds behavior (normally with a couple of minute delay) it will send an email alert, and can be configured to block the host using IPTables or TCPWrappers

Intrusion Detection

- Other Options:
  - Denyhosts - http://denyhosts.sourceforge.net
    - Similar to fail2ban, relies on scripts to parse logs and insert rules when bad behavior is detected
  - OSSEC - http://www.ossec.net
    - Client/Server based system that can be used to watch multiple hosts.
    - Detects bad behavior from log files, can also be used to watch for anomalies such as disk failure, user behavior, interface promiscuousness, and installation of software.
  - Snort - https://www.snort.org
    - System capable of real time analysis and prevention of attack vectors through the use of heuristics
- There are many more pay and free options in this space, look around and choose what makes you comfortable.

Rootkit Detection

- There are two solutions that are typically used to search a host for infections (e.g. ‘rootkits’)
  - These are ‘last resort’ tools normally
  - Remember that a skilled cracker (e.g. not a script kiddie) will cover their tracks – making a rootkit detector required to determine damage
- If you have a fear that you were compromised, or just want to run one of these scanners in the background and have it mail you periodic reports, they can provide useful information:
  - http://rkhunter.sourceforge.net
  - http://www.chkrootkit.org

Logging

- Central logging helps you pull all the data from the perfSONAR node to some other location for analysis
  - Helps track faults
  - Helps watch for mischief
- There are also numerous solutions in the central logging space.
  - Many are free, some are not
  - Some have GUIs and can aggregate lots of hosts
  - Shop around and test things out – some have features you may never need. Sometimes just setting up ‘syslog-ng’ and forwarding to a central host is sufficient
- Some options:
  - http://logstash.net
  - http://www.elasticsearch.org/overview/kibana/

perfSONAR

Host Security

ESnet ENERGY SCIENCES NETWORK
GÉANT
INDIANA UNIVERSITY
INTERNET2®
UNIVERSITY OF MICHIGAN

Securing your perfSONAR host

- The following slides are some well known techniques for making a Linux host more secure
- Some of these are already configured if you do a ‘toolkit’ install, and some are under consideration for the next release
- These slides are just a quick overview of things to consider

Software Updates

- The perfSONAR toolkit is built on CentOS Linux version 7
  - CentOS uses the '**`yum`**' package management system for software version control
  - Typically you can just run '**`yum update`**' (with root permissions) to bring the system up to date. Do this frequently.

Reasons I upgrade my software
It fixes a compability error
It contains important security fix
I want new cool features
So it i will stop pestering me about the new update
imgflip.com

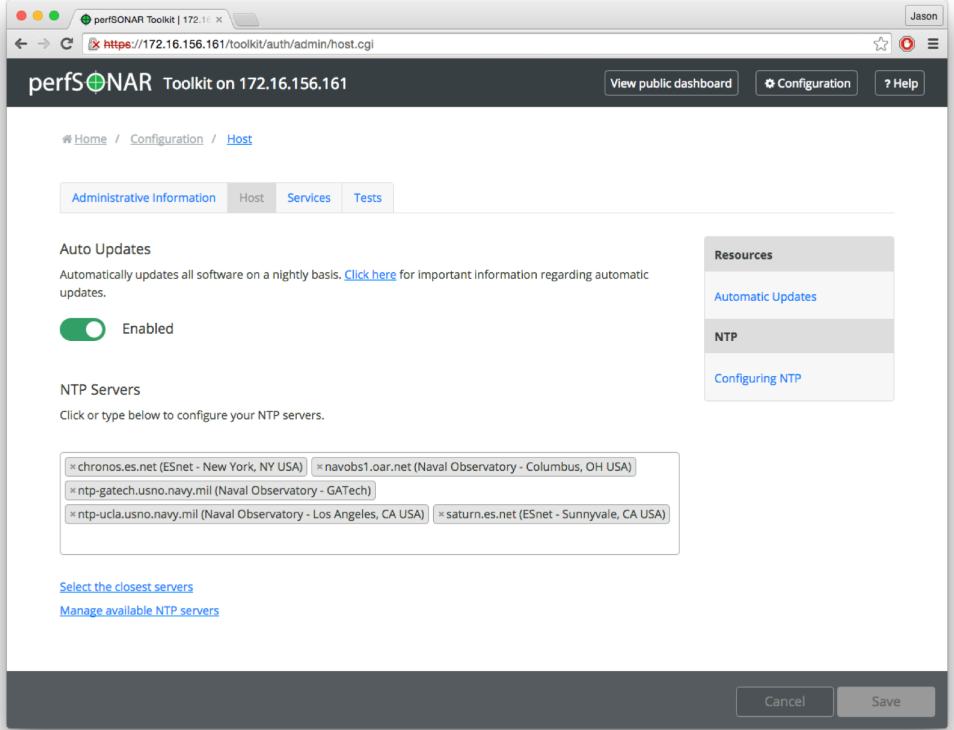
Software Updates

- For some years now, we have an auto-update feature now available:
  - http://docs.perfsonar.net/manage_update.html#automatic-updates
  - Auto-updates will pull down packages from upstream, nightly, to ensure the system stays up to date.
- Obligatory Pro/Con Discussion:
  - Auto-updates are one factor in host security, they are not a panacea. They are also not an excuse to ignore the server exists.
  - Some updates (e.g. kernels) would need a reboot
  - Pulling down updates immediately can sometimes lead to situations where things break (e.g. CentOS or perfSONAR broke something upstream).
    - But developers usually react quickly.

Updates

- Automatic updates via ‘Enabled Services’:

  Note – this is not the end all solution, but it will grab critical things as they come in.


perfSONAR Toolkit | 172.1
https://172.16.156.161/toolkit/auth/admin/host.cgi
Jason
perfSONAR Toolkit on 172.16.156.161
View public dashboard
Configuration
? Help
Home / Configuration / Host
Administrative Information
Host
Services
Tests
Resources
Automatic Updates
NTP
Configuring NTP
Cancel
Save

Auto Updates

Automatically updates all software on a nightly basis. Click here for important information regarding automatic updates.

Enabled

NTP Servers

Click or type below to configure your NTP servers.

× chronos.es.net (ESnet - New York, NY USA)
× navobs1.oar.net (Naval Observatory - Columbus, OH USA)
× ntp-gatech.usno.navy.mil (Naval Observatory - GATech)
× ntp-ucla.usno.navy.mil (Naval Observatory - Los Angeles, CA USA)
× saturn.es.net (ESnet - Sunnyvale, CA USA)

Select the closest servers

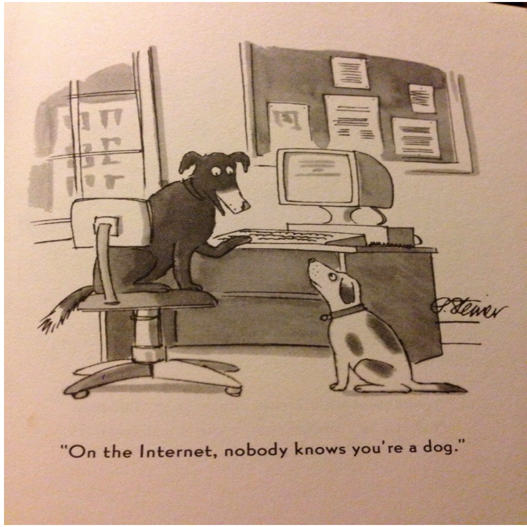
Manage available NTP servers

Software Auditing

- The perfSONAR Toolkit installs only packages that are required for perfSONAR
    - a minimal Linux install plus network monitoring tools
- Some sites may decide they don't need all of these features – if this is the case it may be worthwhile to conduct a software audit
    - `yum list installed`
    - `yum remove packageName`
- Note that `yum` can process dependencies too – if you notice that removing something you don't think is necessary will delete things that are necessary, rethink that choice ☺
- For example, you don't intend to use XWindows on the server, remove it:
    - `yum groupremove "X Window System”`

User Accounts

- perfSONAR can be used in three main ways:
  - Users can view results via the web-based interface. Typically an administrator will have to configure the tests on the machine
  - External users can invoke tests against a perfSONAR machine to the measurement daemons
  - Those with shell accounts can log in, and perform tests/administer the machine (depending on permissions)



- Of these, granting shell access to the machine is the riskiest to deal with
- Some questions to consider when granting a shell account to someone:
  - What are they going to use it for?
  - Will they be an admin, or just a user?
  - Are they a trusted user at the institution?
  - Is the host linked to any other critical institutional resources?

Use of sudo

- The perfSONAR Toolkit also features the **`sudo`** tool that allows someone with ‘administrator’ privileges (set up when accounts are created) to invoke root level access
- By default we allow people in the ‘wheel’ group the ability to run sudo
- Some changes can be made to secure this greater in the **`/etc/sudoers`** file:
  - Require password with each command
    - Change **`ALL=(ALL)        NOPASSWD: ALL`** to be **`ALL=(ALL): ALL`**
  - Limit the commands that can be run via sudo (see file for details)

Centralized Authentication

- If you site already uses this on servers, it can be extended to the perfSONAR Toolkit as well (its just Linux after all …)
  - Typical auth systems are LDAP or Kerberos
- Follow the instructions for setting up this type of system, and finding the correct packages. These documents will be better than what perfSONAR can produce.
- Note – this is non-standard, but can be done if your site has policies that govern the use of this type of system.

Tightening Machine Access

- SSH should be the only login protocol that is running.
- There are some basic SSH protections worth considering:
  - Disable root login in **`/etc/ssh/sshd_config`** (restart the service after doing this)
    - **`PermitRootLogin no`**
  - Allow specific users in **`/etc/ssh/sshd_config`** (restart the service after doing this)
    - **`AllowUsers alice bob`**
  - Disable old protocols **`/etc/ssh/sshd_config`** (restart the service after doing this)
    - **`Protocol 2`**
  - It is also possible to run SSH on a non-standard port:
    - **`Port 2345`**
    - Note that if you take this step, ensure that selinux knows about the change (see **`semanage`**) and that the proper port is open in IPTables (if you are using it).

Tightening Machine Access

- SSH Throttling can be installed into IPTables to prevent brute force attacks:
  - `# Throttling of SSH`
  - `-A INPUT -p tcp --dport 22 --syn -m limit --limit 1/m --limit-burst 3 -j ACCEPT`
  - `-A INPUT -p tcp --dport 22 --syn -j DROP`
- If there are concerns about the use of passwords, you can require public key authentication.
  - This will require all users to generate a public/private key pair and authenticate to the machine in this manner.
  - The following change can be made to `/etc/ssh/sshd_config` (restart the service after doing this)
    - `# Disable password authentication forcing use of keys`
    - `PasswordAuthentication no`
- Lastly, you can limit the exposure of SSH (via IPTables) to ranges of hosts
  - Allow only specific subnets to access or a ‘bastion’ host

Physical Security

- Lets say your server is in a bad neighborhood, it makes sense to protect the physical access.
    - Configure the BIOS to prevent booting from external devices (e.g. USB, CD, etc.)
    - Set the BIOS bootloader password
- If the server is set up for serial access, don't leave root logged into the console (no-brainer …)

Auditing Services

- The default settings for the perfSONAR Toolkit will only enable essential services.
- If you are interested in disabling services you have no intention of using, try the following:
  - `chkconfig --list | grep '3:on’`
  - To disable service, enter:
    - `service serviceName stop`
    - `chkconfig serviceName off`
- Similarly, you can view the services that are in a listening state on the host like this:
  - `netstat –tulpn`
  - Also can use netmap, from an external host:
    - `nmap -sT -O localhost`
    - `nmap -sT -O server.example.com`

Security Scanning

- The use of a vulnerability scanner on a regular basis is an important tool.
  - By doing this, you can see if there are any exposed risks via the software on your machine
  - perfSONAR runs a scan with each major release for default settings – the use of other tools or modifications may change the risk vectors for a machine.
- There are lots of scanners, two popular ones:
  - http://www.tenable.com/products/nessus
  - http://www-03.ibm.com/software/products/en/appscan
- In the general case, any similar implementation will do the same thing – generate a report of categorized warnings for a given vulnerability set.

Outline

- Introduction & Overview
- Security
  - Software Updates & Accounting
  - User Accounts & Machine Access
  - Physical Security
  - Service Audit
  - Firewalls & IDSs
  - Logging
- Conclusions

Conclusions

- A perfSONAR server should requires the same amount of “care and feeding” as any server
  - Yum auto-updates help a lot, but need to make sure they are set them up correctly
  - General server best practices are sufficient
  - Use external monitoring when you can to watch for bad behaviors
- Security is only as advanced as you are willing to make it.
  - Use of external tools, or the audits that you perform, can be a strong defense.
  - If no effort is put in, be prepared to treat the machine as disposable (e.g. do you want ‘pets’ or do you want ‘cattle’)
    - In the disposable case – you certainly don’t want to integrate the machine into your environment very tightly
- There is no magic pill in this space
  - If someone wants to get in, odds are they have a lot more resources than you do to make it so
  - perfSONAR nodes are public and have been compromised before
- Spend some time talking to the right people at your campus about expectations and realities, and then make a plan.

Node Maintenance: Security & Operational Concerns

Event

Presenter, Organization, Email
Date