



Open Source, Compliance & You!

Bill Mathews

ISACA

01/21/2010

Open Source, Compliance & You

Problem: You have a lot of compliance requirements staring you in the face. You don't have a lot of budget and you want to be able to sleep at night.



ENTER OUR
HEROES---



Nagios[®]
Copyright (c) 1999-2008 Ethan Galstad

- Free as in Freedom
- Sometimes Free as in Beer
- Allows for transparency
- Can be more robust than commercial software
- Not just a “knock-off” of commercial software



IF YOU'RE NOT AT
LEAST TRYING FREE
AND OPEN SOURCE
SOFTWARE

I
CAN ONLY USE
WINDOWS, ORACLE
AND EXCHANGE TO
KEEP MY JOB



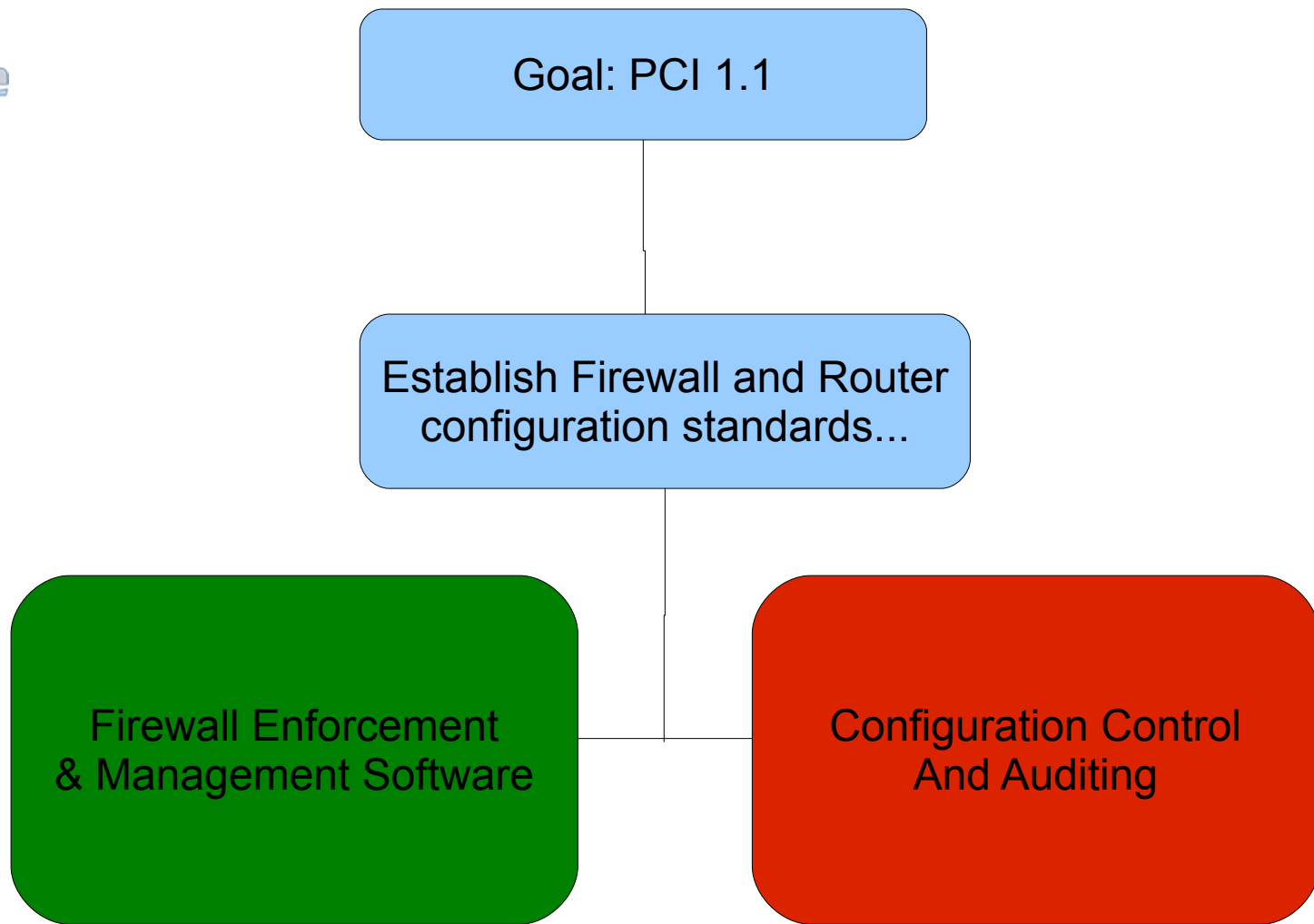
YOU'RE ROBBING
YOUR COMPANY
BLIND!



- Lots of bad ones
- Lots of good ones
- Hard to tell the difference
- Hard to tell where a lot of tools would fit in



I crash a lot and am really
hard to train



Software: Firewall Builder

Tags: Firewall Configuration Management,
PCI 1.1

Info: www.fwbuilder.com

Community: Active

Licensing: Dual

Features: Supports a variety of firewalls
Deploys configuration to firewalls

Maturity: Stable

Software: NCAT: Network Config
Audit Tool

Tags: Firewall Configuration Audit,
PCI 1.1

Info: <http://ncat.sourceforge.net>

Community: Active

Licensing: Free

Features: Audits configuration for security

Maturity: Stable

- By tagging our selected projects carefully we can easily associate them with many compliance goals
- The color coding is just there to differentiate the category of the tool for this compliance goal
- One tool can fit many different goals so its important to tag as meticulously as possible

Tag Library

- Clear concise tags
 - Web Application Firewall is better than Web Filter
- As it relates to compliance goals - more is better
 - If you can use a tool in more than one goal, then tag it appropriately

The “Sniff” Test

- 1) Does the project have a community around?
 - A) Are there mailing lists, forums or newsgroups around the project?
 - B) Are those active?
- 2) Is the project actively maintained?
 - A) When was the last release?
 - B) Are there development releases?
- 3) Google around for the project and see what comes up. It's a very effective method.

More than Sniffing

- You should audit the project yourself (or have some trusted 3rd party to do so
- How to make that happen?

More than Sniffing

- Put the project in the cone of silence!
- Build a test environment!
- Audit the code!
- Test new releases



Cone of Silence

- ✓ Build a lab (Virtualization is acceptable here)
- ✓ Install the software
- ✓ Run the software as you would in production
- ✓ **MONITOR THE LAB ENVIRONMENT**
- ✓ Watch for bad/unexpected/bad to you stuff

Audit the Code!

- Quite a few automated tools do this
- Automated tools are great for finding “low hanging fruit”
- Manual audits or behavioral audits are best

Test New Releases

- You should always, always always test new releases of code
- AND new features!

What to do when it smells funny?

- It's important to keep this list up to date
 - When a project goes unmaintained for 6 months, drop it
 - When a project closes its source, re-evaluate it
 - When a project has more than 5 unresolved security issues, drop it
 - Re-evaluate often

Proof of Concept

<http://www.oscompliance.com>

NCAT – Network Config Audit Tool

Software: NCAT – Network Config Audit Tool

Info: <http://ncat.sourceforge.net>


Community: Moderately Active

Licensing: Free

Features: Automatically fetches config files, audits them based on pre-defined rules, generates reports

Maturity: Stable

News:

×
powered by 

[Web](#) [Blog](#) [News](#) [Book](#)

[NCAT – Network Config Audit Tool Homepage](#)

This is the homepage for development versions of **NCAT**, the **Network Config Audit Tool** and **RAT**, the Router **Audit Tool**. They were written to facilitate ...

ncat.sourceforge.net

[Network Auditing | Configuration Management |](#)

IT Sentinel uncovers latent **network configuration** issues that could cause ... through traditional string matching techniques used by most **auditing tools**. ...

www.opnet.com

[Network Configuration Management Introduction |](#)

Feb 20, 2009 ... **Network configuration** management provides the **tools** to give you an **audit** trail of changes to your network. It can also make enforcing ...

www.openextra.co.uk

[Towards Automated Auditing for Network](#)

Keywords: **Configuration** changes, **Network** auditing automation. 1. INTRODUCTION ... impact multiple parts of a **configuration**. Existing **auditing tools** ...

www.cs.st-andrews.ac.uk

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)

FWBuilder

Software: Firewall Builder

Info: <http://www.fwbuilder.com>

Community: Active

Licensing: Dual

Features: Supports a variety of firewalls, provides central management to a variety of firewalls, easier, reusable objects

Maturity: Stable - released 2000

News:

powered by 

[Web](#)

[Blog](#)

[News](#)

[Book](#)

[Firewall Builder](#)

Firewall Builder is Open Source multi-platform firewall management software that supports Linux iptables, FreeBSD ipfilter and ipfw, OpenBSD pf, ...

www.fwbuilder.org

[Firewall Builder packages for Windows and Mac OS X](#)

If you purchased license for Firewall Builder 2.1 between July 1 and August 31 of 2008, please contact us at support@netcitadel.com to get your free upgrade ...

www.fwbuilder.org

[Firewall Builder | Get Firewall Builder at SourceForge.net](#)

Get Firewall Builder at SourceForge.net. Fast, secure and free downloads from the largest Open Source applications and software directory.

sourceforge.net

[Firewall Builder](#)

Have you ever wanted to configure a personal firewall for your GNU/Linux box, but were scared of the complexity of iptables? Well, I might not be able to ...

www.freesoftwaremagazine.com

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)

OSSEC – Host Based IPS and System Monitoring

Software: OSSEC – Host Based IPS and System Monitoring

Info: <http://www.ossec.net>

Community: Very Active

Licensing: Free, GPL v3

Features: Actively monitors hosts based on a set of rules (XML), centrally managed, can take evasive actions

Maturity: Stable

News:

 ×

powered by 

[Web](#) [Blog](#) [News](#) [Book](#)

[Welcome to the Home of OSSEC](#)

OSSEC – Open Source Security, Host-Based Intrusion Detection System.

www.ossec.net

[Downloads](#)

Windows agent version 2.3. **OSSEC** for Windows 2000,XP, 2003 and Vista: ... If you find **ossec** useful and would like to contribute back to the community, ...

www.ossec.net

[OSSEC – Wikipedia, the free encyclopedia](#)

OSSEC is a free, open source host-based intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, ...

en.wikipedia.org

[Amazon.com: OSSEC Host-Based Intrusion Detection Guide](#)

Amazon.com: **OSSEC** Host-Based Intrusion Detection Guide (9781597492409): Andrew Hay, Daniel Cid, Rory Bray: Books.

www.amazon.com

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)

Hurricane Labs References:

http://www.hurricanelabs.com/january2008_story_2

<http://news.hurricanelabs.com/article.php?story=20071211101538488>

OSSEC – Host Based IPS and System Monitoring

Software: OSSEC – Host Based IPS and System Monitoring

Info: <http://www.ossec.net>


Community: Very Active

Licensing: Free, GPL v3

Features: Actively monitors hosts based on a set of rules (XML), centrally managed, can take evasive actions, can be used

Maturity: Stable

News:

×
powered by 

[Web](#) [Blog](#) [News](#) [Book](#)



[OSSEC v2.3 released](#)

Dec 07, 2009

We are very happy to announce that general availability of **OSSEC** version 2.3 (just in time for the holidays). What is new? Log analysis rules for the Nginx web server; Log analysis rules for Suhosin (Hardened PHP); Support for real time ...

<http://www.ossec.net/?q=Save+Us+From+Berlusconi>

[OSSEC 2.3 released](#)

Dec 09, 2009

OSSEC 2.3 was actually released a few days ago, but a careful reader pointed out we had not covered it yet. From the announcement: What's New? Log analysis rules for the Nginx web server; Log analysis rules for Suhosin (Hardened PHP) ...

<http://isc.sans.org/>

[Cloud Security & Adoption Realities: OSSEC survey says...](#)

Dec 18, 2009

OSSEC is an Open Source Host-based Intrusion Detection System project that has been around since 2003. It was acquired by Third Brigade in 2008, and then Third.

<http://cloudsecurity.trendmicro.com/>

[Week of OSSEC](#)

Oct 31, 2009

As a service to the community and to coincide with my speaking on **OSSEC** at the Rochester Security Summit, every day during the week of October 25 through October 31, I'll be posting a new tip on **OSSEC** based on my years of first-hand ...

<http://www.ossec.net/?q=http://www.evilliv3.org/>

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)

Hurricane Labs References:

http://www.hurricanelabs.com/january2008_story_2

<http://news.hurricanelabs.com/article.php?story=20071211101538488>

FWBuilder

Software: Firewall Builder

Info: <http://www.fwbuilder.com>

Community: Active

Licensing: Dual

Features: Supports a variety of firewalls, provides central management to a variety of firewalls, makes host firewalls easier, reusable objects

Maturity: Stable - released 2000

News:

x
powered by 

Web Blog News **Book**



[How to Cheat at Securing Linux](#)

by James Stanger
2007 - 415 pages
books.google.com



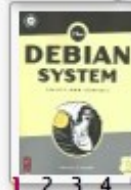
[Troubleshooting Linux firewalls](#)

by Michael Shinn, Scott Shinn
2005 - 369 pages
books.google.com



[Linux Firewall: Schnellkonfiguration ; \[der](#)

by Till R. Dierkesmann
2006 - 224 pages
books.google.com



[The Debian system: concepts and](#)

by Martin F. Krafft
2005 - 605 pages
books.google.com

1 2 3 4 5 6 7 8

Build Your Own!

- I built this archive with very little effort
- Build your own archive of “blessed” tools for use in achieving compliance goals
- Providing this sort of guidance can and will be invaluable to your organization



<commercial>

Don't want to do this all yourself? Call Hurricane Labs. Our Hurricane Defense Service blends the best of these tools with our integration technology for an Open Source experience you won't believe.

</commercial>

Q & hopefully A



Thank you for your time