Are we <insert here> compliant?

configuration auditing from an engineer's perspective

Chad Streck, Staff Research Engineer @ Tenable, Inc.
GRASSr00tz - June 9, 2022

Disclaimer

This is not meant to be a vendor presentation. Yet my experience is with a very specific product, so please excuse vendor specific items.

Goal

Give a mid-high level explanation of configuration auditing, techniques used, and how it relates to policy compliance.

We all know Vulnerability Scanning

Process of identifying security weaknesses and flaws in systems and software running on them.

- Primarily check versions and patch levels.
- Inspect active processes and connections for IOC. (hashes, names, metadata)
- Test (non-disruptively) known vulnerabilities.
- Alerts raised based on **severity** of found vulnerabilities.
- Lots of process and standardization in CVE and CVSS.

Reactive

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

What is configuration auditing?

Examination of the as-built configuration of systems as compared to its implementation.

- Check configurations as they match to expected policy.
- **Automate the technical checks**.
- All recommendations tested and reported as binary; **PASS** and **FAIL**.
- Attempts of standardization in CCE and CCSS, but is reliant on organizational policies.

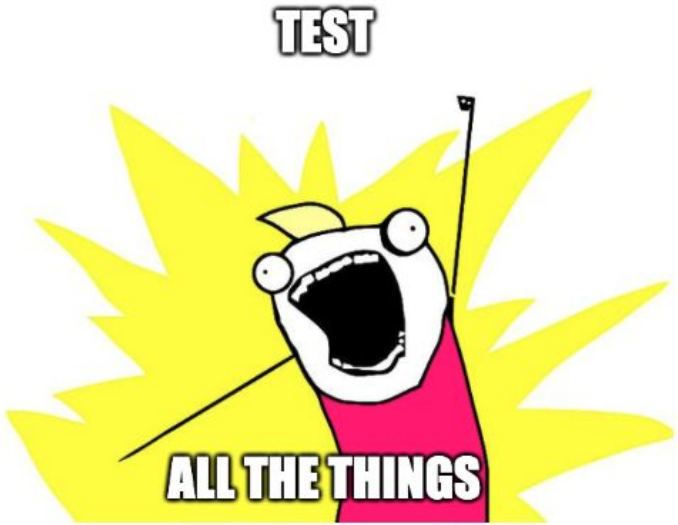
Proactive

The Technical

What to test

Different aspects to test a configuration.

- Should be - IaC, MDM, GPO
- On disk - Configuration files and settings
- As started - Initialization files and settings
- As running - Active processes



Best to test all… but may not be feasible due to time, resources, complexity....

Gather -> Transform -> Evaluate

Process for testing all recommendations.

Gather

- Host - Process on host searches for files, registry settings, processes,...
- Remote - Same as host, but over a network connection.
- Offline - Someone else has already gathered the required data.
- Management - MDM and other systems that push values
- Cloud - Connect to cloud management systems and pull the configuration.
- Code - Evaluate configurations before they are instantiated.

Gather -> **Transform ->** Evaluate

Transformation of different formats into a normalized format that is easily evaluated.

Transform

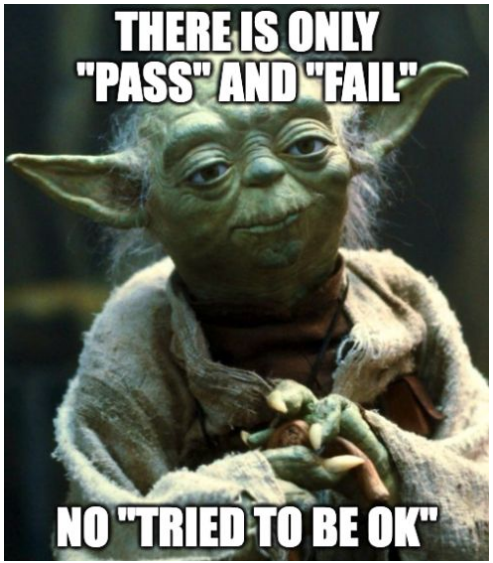
- File contents - filtered (grepped) to lines, or searched for content.
- XML and JSON data - many times converted to targeted text.
  - Large list of data transformed to single item per data point.
  - Pull out a very specific value.
- Process and File metadata has to be presented in a consistent format.
- Code - normalized and transformed to a consistent format.

Gather -> Transform -> **Evaluate**

Here is where the tires hit the pavement.

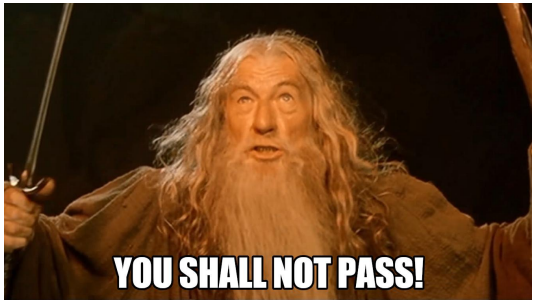
Evaluate

- Exact match.
- Value exists in list
- Value does not exist
- Value in range



All result in a **PASS** or **FAIL**.

Examples



Linux - SSH server should not allow Root logins

- **Gather** - get contents of “/etc/ssh/sshd_config” file
- **Transform** - find only the line that looks like “PermitRootLogin…”
- **Evaluate** - verify it is set to “no” by matching “PermitRootLogin no”

Windows -Dialog box title for the legal banner must be configured.

- **Gather** - retrieve registry value at …

```
HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption
```

- **Transform** - No need to transform
- **Evaluate** - verify it matches organizational value of “You Shall Not Pass!”

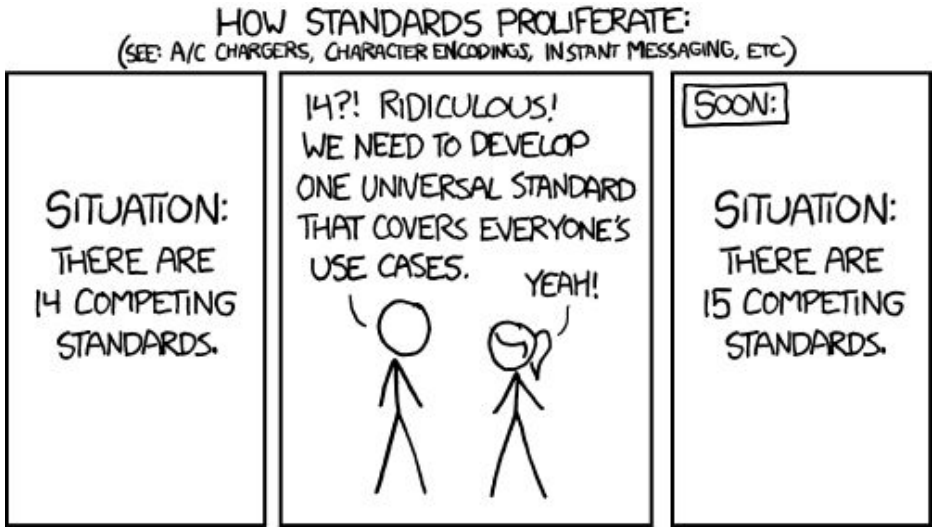
The Policy

Standards

Standards are recipes that list out requirements that organizations must meet.

- Stay very high level in defining what must be done.
- Can be as general as “must do the security”.
- If aligned with a regulation, will be legally binding.

Examples: PCI-DSS, GDPR, SOX, NERC CIP, HIPAA, ISO 27001...



https://xkcd.com/927/

Frameworks

Frameworks are series of documented processes that are used to define policies and procedures.

- More prescriptive, but still general.
- Provides starting a starting point to define organizational policies

Examples: NIST 800-53, NIST 800-171, NIST CSF, CIS CSC, CSA CCM, OWASP, ...

NIST 800-53

SC-44 Detonation Chambers

The organization employs a detonation chamber capability within *[Assignment: organization-defined information system, system component, or location]*.

Benchmarks and Guides

Where the rubber hits the road.

Enumerates the recommendations to secure a system.

Each recommendations will describe ...

- What configuration to make.
- Why making the configuration is secure.
- How to check for the proper configuration.
- How to properly set the configuration.

Popular Configuration Guides

CIS - Center for Internet Security

- **Security Benchmarks**
- Community driven working groups.
- https://www.cisecurity.org/cis-benchmarks/

DISA - Defense Information Systems Agency

- **Security Technical Implementation Guides**
- Any and all US government contractors working with DoD must comply.
- https://public.cyber.mil/stigs/

Example: What and Why

The Windows dialog box title for the legal banner must be configured.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-63681	WN10-SO-000080	SV-78171r1_rule		Low

Description

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

STIG	Date
Windows 10 Security Technical Implementation Guide	2016-11-03

Example: How and How

Check Text (C-64427r1_chk)

Search...

If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\

Value Name: LegalNoticeCaption

Value Type: REG_SZ
Value: See message title above

"DoD Notice and Consent Banner", "US Department of Defense Warning Statement" or a site-defined equivalent, this is a finding.

If a site-defined title is used, it can in no case contravene or modify the language of the banner text required in WN10-SO-000075.

Fix Text (F-69609r1_fix)

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Message title for users attempting to log on" to "DoD Notice and Consent Banner", "US Department of Defense Warning Statement", or a site-defined equivalent.

Example: Coverage of a Secure System

CIS Ubuntu Linux 20.04 LTS STIG Benchmark 1.0.0

1 - Initial Setup

2 - Services

3 - Network Configuration

4 - Logging and Auditing

5 - Access, Authentication and Authorization

6 - System Maintenance

Crosswalk

A map between coding systems. Coding systems here are various standards and frameworks.

CSCv8 8.5 - Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation

NIST 800-53 AU-3 - The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

GDPR 32-1(b) - Security of Processing: the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

HIPAA 164.312(b)- Technical safeguards Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

NIST CSF PR.PT-1 - Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Creating a Secure Policy

- Start with a benchmark/guide.
- Modify to meet your organizational needs
- Crosswalk to the standard or framework to align with
- Evaluate sufficiency to the standard or framework
- Identify and document where you have compensating controls
- Fill in any missing data using additional configuration audits or manual collection and evaluation.

Bottom-up Approach

The Future

Future Trends

If I had a crystal ball….

Technical

- More focus on IaC auditing to keep moving left.
- Methods to store configuration values to provide offline auditing and “What If” scenarios

Policy

- Improved prioritization using concepts of implementation groups.
- Organizational Top-Down approach to policy creation

Are we <insert framework> compliant?

Maybe, maybe not, is there enough information…

- Technical controls are tested, but is everything tested?
- Non-technical controls are not, but could be by survey?
- Compensating controls can… compensate, or recast results.

Auditors have job security.

Configuration auditing will provide the data that the automatable tests have been done and evaluated, confidence that no major changes have been introduced, along with collected data that can be evaluated by humans.

Thank You