Automating security compliance for physical, virtual, cloud, and container environments

Using Red Hat CloudForms, Red Hat Satellite, Red Hat Insights and Ansible Tower by Red Hat

Lucy Huh Kerner
Principal Technical Marketing Manager - Security, Red Hat
May 4, 2017
Why automate security compliance?
“81% of hacking-related breaches leveraged either stolen and/or weak passwords.”

2017 Verizon Data Breach Investigations Report
Let’s manually ensure security compliance …..

● 3 ring binder of security checks and fixes that have to be done
● Very time consuming
● Highly prone to human error
● Tedious and boring
● Non-repudiable
● Not easy to do audits
● Not repeatable or sharable
Instead, what you want is ...

● Centralized management of your **entire** heterogeneous infrastructure
  ○ You can’t control what you don’t know about
● Automation, Automation, Automation
● Infrastructure and Security as code
  ○ Repeatable, sharable, verifiable, easier to do compliance audits
● Hardened, Security compliant host at provisioning time
  ○ Immutable Operating System: OS can’t be changed by untrusted parties
● Automated monitoring and fixing of all systems for entire lifecycle
● Proactive vs Reactive security
What tools can I use to help me with all this?
Let’s start with SCAP. But, what is SCAP?

- Security Content Automation Protocol
- Managed by National Institute of Standards and Technology (NIST)
- Standardized way of maintaining security of systems
  - Vulnerability and configuration security baselines
WHAT IS OpenSCAP?

NIST validated and certified SCAP scanner by Red Hat

Security Content Automation Protocol (SCAP) 1.2 Product Validation Record

- **Validation Number:** 142
- **Vendor:** Red Hat®, Inc.
- **Product Name:** OpenSCAP
- **Product Major Version:** 1
- **Product Version Tested:** 1.2.13
- **Tested Platforms:**
  - Red Hat Enterprise Linux 6.8 Client, 32 bit (x86)
  - Red Hat Enterprise Linux 6.8 Client, 64 bit (x64)
  - Red Hat Enterprise Linux 7.2 Client, 64 bit (x64)
- **SCAP 1.2 Capabilities:**
  - Authenticated Configuration Scanner
  - Common Vulnerabilities and Exposures (CVE)
  - Validated Product
  - Vendor Provided SCAP Information
- **Dates Tested:**
  - 11/22/2016 12:00:00 AM - 2/7/2017 12:00:00 AM
- **Report Submitted:**
  - 2/8/2017 12:00:00 AM
- **DTR Version:** NIST IR 7511 Revision 4
- **Validation Test Suite:**
  - version 1.2.0.0.0 (December 2012 release includes R600-1.2.0.0.1, R1900-1.2.0.0.2, R3300-1.2.0.0.3 out of cycle updates)
  - version 1.2.0.1.0 (August 2013 release)
  - version 1.2.0.2.0 (March 2014 release)
  - version 1.2.0.3.0 (April 2015 release)
  - version 1.2.1.0.0 (April 2016 release)
  - version 1.2.1.1.0 (June 2016 release)
- **Previous Validation:**
  - SCAP 1.2
- **SCAP and Product Version:**
  - OpenSCAP Version 1.0.8-1.el5_10 (Validation Record Number 128)
  - NVLAP Lab: 200416-0 - COACT
- **Validation Date:**
  - 2/22/2017 12:00:00 AM

**Note:** The vendor assertions document (aka Vendor Provided SCAP Information) was provided by the vendor. The descriptions do not imply endorsement by the U.S. Government or NIST.
PRESS RELEASE

Red Hat Adds New NIST Certification for OpenSCAP, Expands Footprint for Open IT Security Standards

Community-driven security compliance scanner certified for mission-critical deployments on Red Hat Enterprise Linux 6 and 7 by National Institute of Standards and Technology

RALEIGH, N.C. — March 17, 2017 — Red Hat, Inc. (NYSE: RHT), the world’s leading provider of open source solutions, today announced that OpenSCAP 1.2, an open source Security Content Automation Protocol (SCAP) scanner, has been certified by the National Institute of Standards and Technology as a U.S. government evaluated configuration and vulnerability scanner for Red Hat Enterprise Linux 6 and 7-based systems. This certification shows that OpenSCAP can analyze and evaluate security automation content correctly and has the functionality and documentation required by NIST to run in sensitive, security-conscious environments.

“NIST’s new certification of OpenSCAP on the world’s leading enterprise Linux platform provides a flexible, powerful SCAP scanner built on open standards, making it easier for agencies and other organizations to add verifiable, repeatable security scanning to their repertoires.”

DAVID EGTS, CHIEF TECHNOLOGIST, PUBLIC SECTOR, RED HAT
SCAP Workbench

- GUI tool that serves as an SCAP scanner and provides tailoring functionality for SCAP content, but only scans a single machine
But... I don’t just have 1 machine ...  

- We have over 1000 linux hosts all living in different environments (VmWare vCenter, Microsoft Azure, etc). How do we scan, report on, and remediate all of these systems?
- How do we provide a customized self service portal for users to provision a security compliant host at provisioning time while still having tight control over our entire infrastructure?
- How do we do ongoing automated security compliance and remediation for our entire heterogeneous infrastructure?
- How do I ensure that all the 200+ container images in our environment and all future container images that will enter our environment are free of vulnerabilities in an automated fashion?
The secret is to use a combination of OpenSCAP and Ansible Tower by Red Hat.
Using Red Hat’s management products + OpenSCAP, how do I:

1) Create a security compliant host at provisioning time
2) Automate ongoing security compliance
3) Ensure governance and Control
4) Do proactive vs reactive security with Red Hat Insights

**All in a heterogeneous infrastructure with a mix of physical, virtual, cloud, and container environments**
Creating a security compliant host at provisioning time with Red Hat CloudForms and Ansible Tower
Unified Management with Red Hat CloudForms

CONTAINERS
Red Hat® OpenShift Container Platform

VIRTUALIZATION
VMware®, Microsoft® Hyper-V, Red Hat Virtualization

PRIVATE CLOUD
Red Hat Openstack® Platform

PUBLIC CLOUD
Amazon© Web Services, Microsoft Azure, Google© Cloud Platform

SOFTWARE DEFINED NETWORKING
CloudForms includes Ansible Inside (default automation for CloudForms)

**TOWER** EXPANDS AUTOMATION TO YOUR ENTERPRISE.

- **CONTROL**
  - Scheduled and centralized jobs

- **KNOWLEDGE**
  - Visibility and compliance

- **DELEGATION**
  - Role-based access and self-service

- **SIMPLE**
  - Everyone speaks the same language

- **POWERFUL**
  - Designed for Multi-tier deployments

- **AGENTLESS**
  - Predictable, reliable, and secure

AT ANSIBLE’S CORE IS AN OPEN-SOURCE AUTOMATION ENGINE.
DEMO #1
Creating a security compliant host at provisioning time

1. Push an order button in CloudForms which, behind the scenes will:
   ○ Provision a VM in VmWare
   ○ Register it with Satellite

2. Do all this WITHOUT writing a single line of code and WITH multi-tenancy
   ○ Users from different tenants have their own “order buttons”

3. Admin has tight control of entire heterogenous infrastructure and only allows certain people provision in Amazon vs VMWare based on tenancy, utilization, etc
Now, let’s see this in action!
You can also create a security compliant host in RHEL 7.2, RHEL 7.3 + Satellite 6
Of course, can kickstart too or create security compliant host(s) using Satellite 6 as well vs RHEL GUI install.
Automating ongoing security compliance with Red Hat CloudForms, Satellite, OpenSCAP, and Ansible Tower
Automate ongoing security compliance

1. Push a button on a VM in CloudForms and do an OpenSCAP scan on it for a chosen security profile (PCI-DSS, DISA STIG, Standard, etc or your custom profile)
   ○ When the scan PASSES:
     i. Tag the VM as scap-compliant:<name of profile>
   ○ When the scan FAILS:
     i. Tag the VM as scap-noncompliant:<name of profile>
     ii. Email owner of VM
     iii. Open a ticket in a ticketing system, such as ServiceNow with the name of the failed VM and all other details about VM(size, IP address, etc)
2. Create reports of ALL scap-compliant/non-compliant VMs based on security profile
3. Push a button to fix the VM based on security profile. Once that looks good, do the fix for ALL machines in my environment at the push of a button.
Now, let’s see this in action!
The Power and Flexibility of the Red Hat CloudForms control/policy engine
DEMO #3
Power and Flexibility of the CloudForms control engine

1. Check to see if your VM is vulnerable to shellshock. If yes, then fix the VM using a button in CloudForms that launches an Ansible playbook to remediate the VM against the shellshock vulnerability.

2. In CloudForms, check to see if an Openshift container image has any severity high vulnerabilities. If yes, then Openshift will prevent that vulnerable image from ever running in Openshift again.
Now, let’s see this in action!
Proactive Security and Automated Risk Management with Red Hat Insights
Insights introduces automated risk management, reduces complexity, and allows you to **FIX** faster.

- **Ansible** by Red Hat
  - Automate your IT processes & deployments:
    - Simple & powerful language
    - No agents to install
    - Scale with Ansible Tower

- **Red Hat Insights**
  - Prevent critical issues before they occur
    - Continuous Insights
    - Verified Knowledge
    - Proactive Resolution

- **Red Hat Satellite**
  - Build a trusted & secure Red Hat environment
    - Manage the Red Hat lifecycle
    - Provision & configure at scale
    - Standardize your environment

- **Red Hat CloudForms**
  - Deliver services across your hybrid cloud
    - Hybrid cloud management
    - Self-service provisioning
    - Policy-driven compliance
1. See the payload injection issue on your VM in Red Hat Insights from either Satellite or CloudForms.
   ○ Upon fixing, notice that the issue no longer exists
Now, let’s see this in action!
SUMMARY

1) Create a security compliant host at provisioning time
2) Automate ongoing security and compliance
3) Ensure governance and Control
4) Do proactive vs reactive security with Red Hat Insights

All with **FLEXIBILITY + CHOICE** using a combination of OpenSCAP, Red Hat CloudForms, Red Hat Satellite, Ansible Tower, and Red Hat Insights
Your only limits are the limits of your imagination...
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews
RED HAT SUMMIT

LEARN. NETWORK. EXPERIENCE OPEN SOURCE.