Security and Compliance Scanning Tool for Containers

Bharath Ananthanarayanan
Blake Hina
Vrushali Mahajan
Ben Owens

OpenScap is an auditing tool to verify whether a system confirms to standards specified in Security Content Automation Protocol (SCAP).

OpenSCAP checks for two features:

Security Compliance: Security compliance is a state where computer systems are in line with a specific security policy.

Vulnerability Assessment: Vulnerability assessment is a continuous process that identifies security flaws and weaknesses in software.

What was already available?

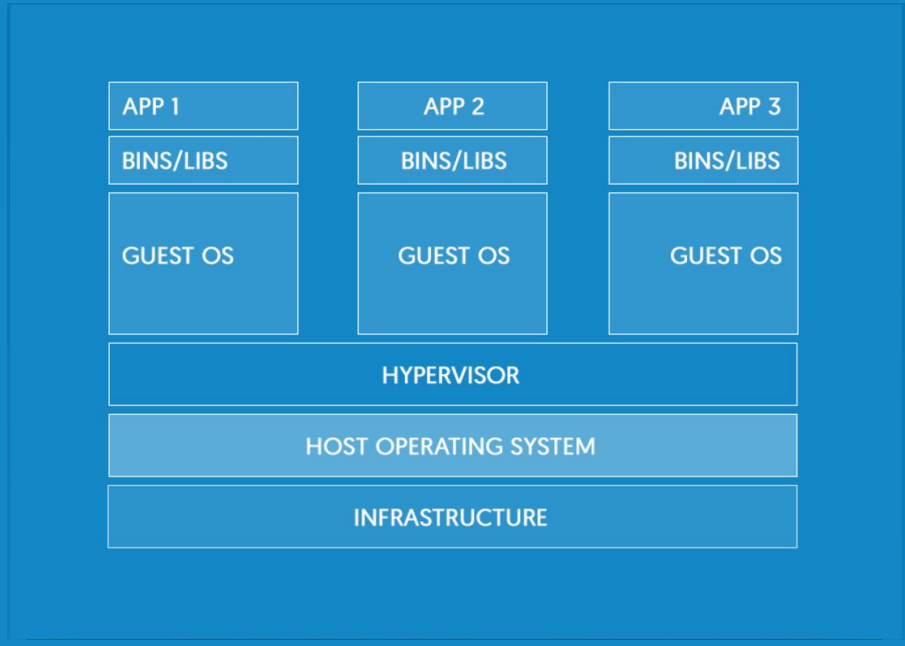
- To scan a system, typically, OpenSCAP tool and security content needs to be installed into the system before scanning it.
- To check vulnerabilities, the tool downloads vulnerability definitions each time tool is invoked.
- OpenSCAP tools support scanning RedHat images and containers without installing tools and content.

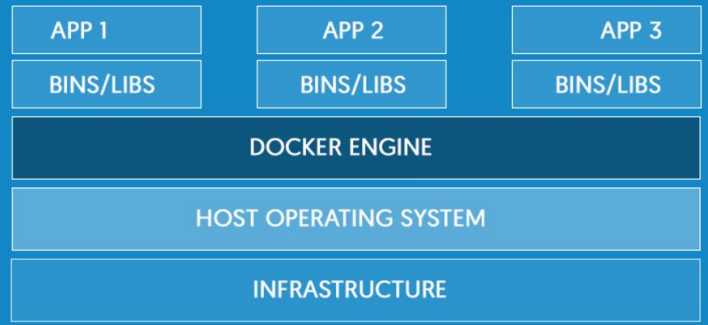
Objective

- The goal of this project to extend this to capability to scan images and containers of other distributions without installing anything on the container.

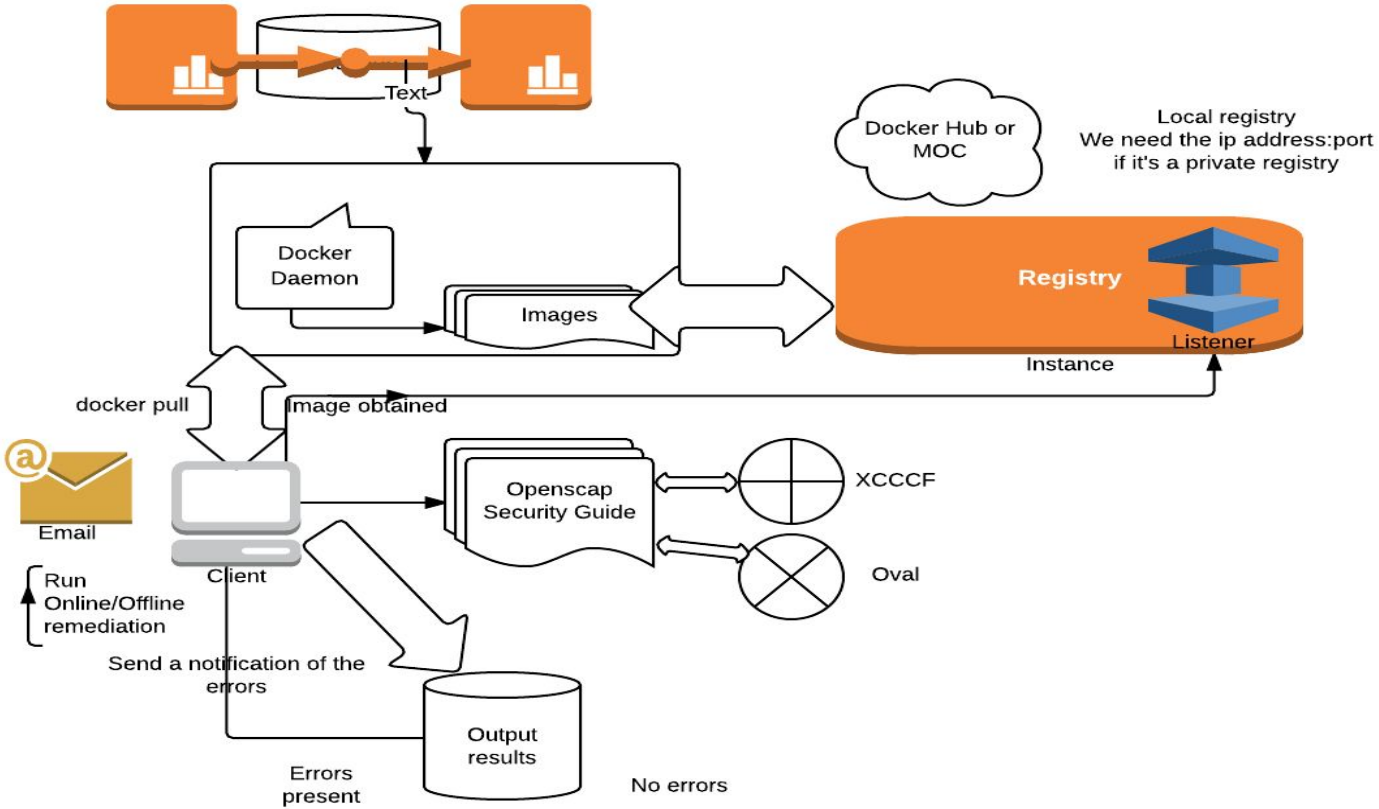
Keywords: *OpenSCAP, vulnerabilities, security content*


docker


APP 1
APP 2
APP 3
BINS/LIBS
BINS/LIBS
BINS/LIBS
GUEST OS
GUEST OS
GUEST OS
HYPERVISOR
HOST OPERATING SYSTEM
INFRASTRUCTURE


APP 1
APP 2
APP 3
BINS/LIBS
BINS/LIBS
BINS/LIBS
DOCKER ENGINE
HOST OPERATING SYSTEM
INFRASTRUCTURE

Architecture



Components of OpenSCAP

- Scanner - an application that reads SCAP security policy and checks whether or not the system is compliant with it
- Security Policy, or “SCAP content” - machine-readable descriptions of the rules which your system will be required to follow
  - Verified policies are available in the SCAP Security Guide
  - Profile - sets of rules and values implemented according to a specific security baseline
- Report - an overview of scan results

Security Policies and Compliance

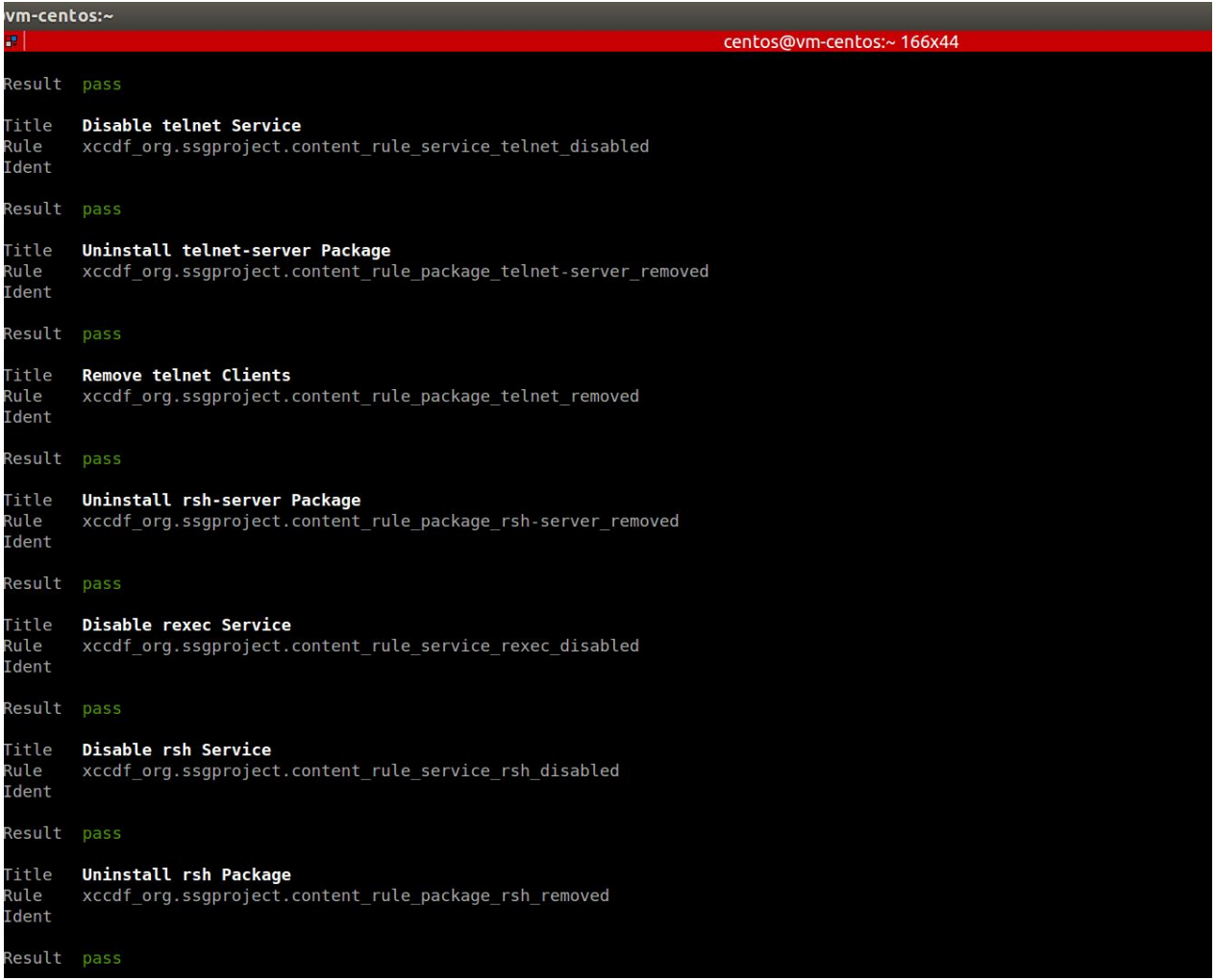
- The system must conform to a set of rules written in machine-readable form.
- Default policies are provided by SCAP Security Guide (SSG) for Fedora, RHEL, CentOS or Scientific Linux..
- The choice of policy mainly depends on what application the infrastructure is used for.
- Eg: If you are working with the US government, you most likely need to comply with USGCB.

Scanning a system

The steps to perform a scan of a system:

1. Selecting a Security Policy present in the SSG
2. Selecting a Profile (a subset of rules)
3. Execute the scan
4. Evaluate scan results

(5.) Remediation


vm-centos:~
centos@vm-centos:~ 166x44
Result pass
Title Disable telnet Service
Rule xccdf_org.ssgproject.content_rule_service_telnet_disabled
Ident
Result pass
Title Uninstall telnet-server Package
Rule xccdf_org.ssgproject.content_rule_package_telnet-server_removed
Ident
Result pass
Title Remove telnet Clients
Rule xccdf_org.ssgproject.content_rule_package_telnet_removed
Ident
Result pass
Title Uninstall rsh-server Package
Rule xccdf_org.ssgproject.content_rule_package_rsh-server_removed
Ident
Result pass
Title Disable rexec Service
Rule xccdf_org.ssgproject.content_rule_service_rexec_disabled
Ident
Result pass
Title Disable rsh Service
Rule xccdf_org.ssgproject.content_rule_service_rsh_disabled
Ident
Result pass
Title Uninstall rsh Package
Rule xccdf_org.ssgproject.content_rule_package_rsh_removed
Ident
Result pass

VULNERABILITY

- A weakness in the software that allows attacker to reduce information assurance.
- VULNERABILITY ASSESSMENT
    - Many software vendors publish their advisories. These typically contain warnings and notifications advising users to update once a fix is available.
    - OpenSCAP uses many such data sources to identify security vulnerabilities present in the system, determine the security impact and consequences of each detected vulnerability perform corrective operations based on this knowledge.

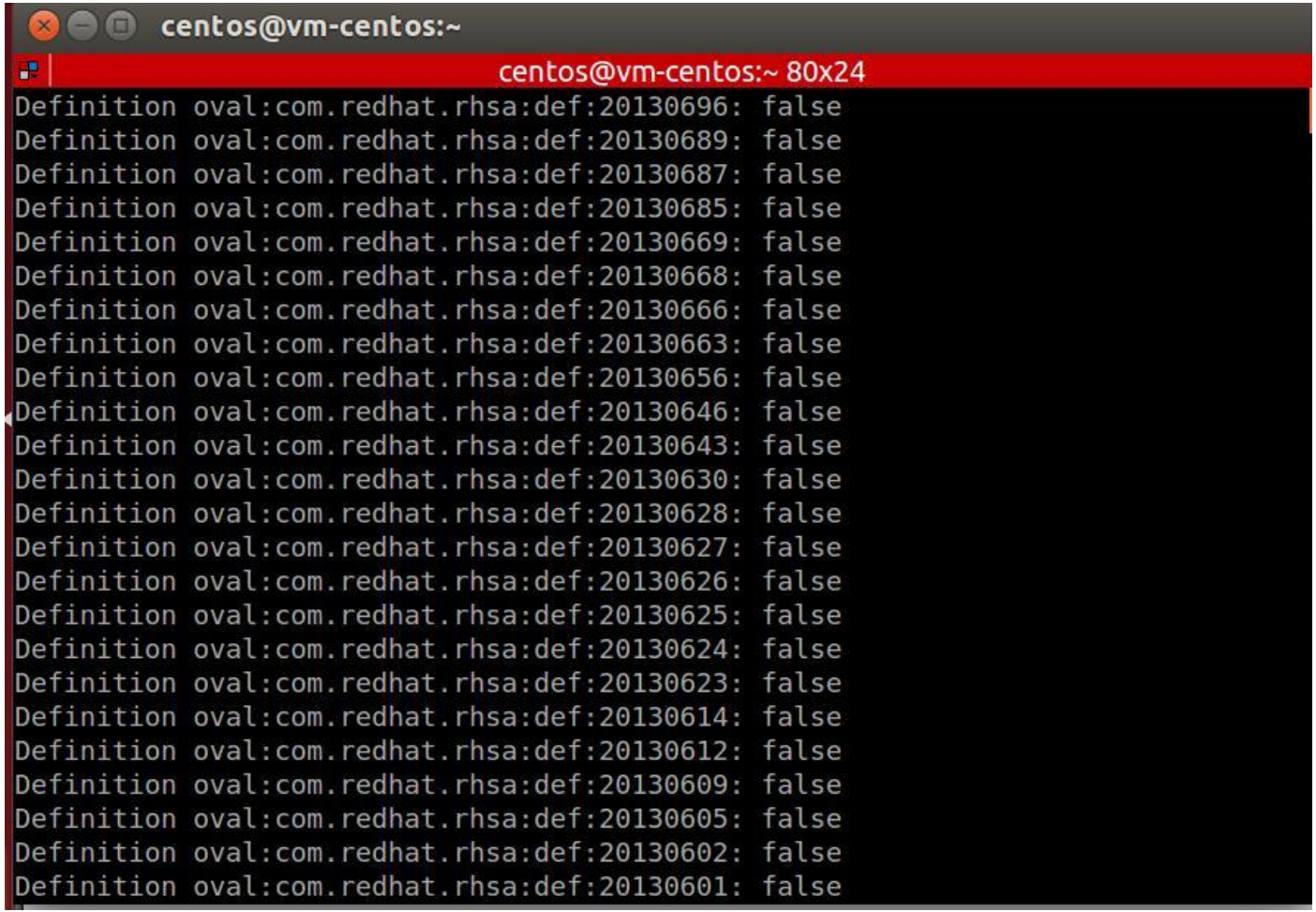
Vulnerability Assessment for a system

There are three steps to perform:

1. Download the file that contains OVAL definitions describing all known vulnerabilities.

2. Execute the oscap tool

3. Review the results


centos@vm-centos:~
centos@vm-centos:~ 80x24
Definition oval:com.redhat.rhsa:def:20130696: false
Definition oval:com.redhat.rhsa:def:20130689: false
Definition oval:com.redhat.rhsa:def:20130687: false
Definition oval:com.redhat.rhsa:def:20130685: false
Definition oval:com.redhat.rhsa:def:20130669: false
Definition oval:com.redhat.rhsa:def:20130668: false
Definition oval:com.redhat.rhsa:def:20130666: false
Definition oval:com.redhat.rhsa:def:20130663: false
Definition oval:com.redhat.rhsa:def:20130656: false
Definition oval:com.redhat.rhsa:def:20130646: false
Definition oval:com.redhat.rhsa:def:20130643: false
Definition oval:com.redhat.rhsa:def:20130630: false
Definition oval:com.redhat.rhsa:def:20130628: false
Definition oval:com.redhat.rhsa:def:20130627: false
Definition oval:com.redhat.rhsa:def:20130626: false
Definition oval:com.redhat.rhsa:def:20130625: false
Definition oval:com.redhat.rhsa:def:20130624: false
Definition oval:com.redhat.rhsa:def:20130623: false
Definition oval:com.redhat.rhsa:def:20130614: false
Definition oval:com.redhat.rhsa:def:20130612: false
Definition oval:com.redhat.rhsa:def:20130609: false
Definition oval:com.redhat.rhsa:def:20130605: false
Definition oval:com.redhat.rhsa:def:20130602: false
Definition oval:com.redhat.rhsa:def:20130601: false